ELECTRONIC LITERATURE DIRECTORY

Individual Work
Redshift and Portalmetal

Redshift and Portalmetal, by micha cárdenas, is an enigma. It is a hypertextual, dystopian sci-fi adventure game. It is a multi-genre, choose-your-own-adventure story blending short fiction, poetry, memoir, and performance art. It is a transreal exploration of the self as a nexus of overlapping and conflicting identities. It is a meditation on climate change and the neocolonial engine that drives it. Echoing Octavia Butler, Redshift compels us to see legacies of colonialism as they pollute the air, degrade our communities, become mapped onto our bodies, but it also asks us to imagine an alternative future, one in which we might resist the urge to colonize as we seek out new worlds for human habitation. In so doing, we begin to imagine what it might mean to decolonize this planet. Ultimately, Redshift is really a story about re-birth, for the planet, for the self. It is a rejection of the conventions that reinforce colonial ideology. It is also a call for solidarity, intersectionality, and agency for people whose experiences and lifeways have for centuries been chewed up by the machine of power, particularly indigenous peoples who are purposefully honored in this project.

As we enter the world of Redshift, we are faced with a truth: “Your planet is dying.” cárdenas’s use of second-person positions the reader in the body of Roja, a trans person of color who must leave her planet in order to survive. The narrative shifts back and forth between second and third person, calling on us to follow Roja’s story, but also to occupy her consciousness. We are (with) Roja as she realizes she must leave. We make decisions about how to traverse space between three settings: the Ice Planet, the Planet with No Rain, the Ocean Moon.

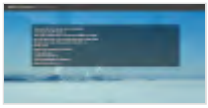
Two devices aid the viewer in coming to identify with Roja and her journey. First, cárdenas presents us with moments where we step out of Roja’s body and see her on-screen (played by cárdenas herself). Seeing Roja’s body we better understand the many identities that she occupies. Her complexity interrupts the voyeuristic impulse that dominates how non-trans people often attempt to understand trans experience. Second, as Roja moves from planet to planet, she must navigate border security. In these spaces, we are faced with anxiety and fear, we are compelled to wait nervously for clearance or to run. At these moments, the story focuses our attention on the precariousness of life at literal and metaphorical borders.

Each planet is depicted via full-screen video with text overlaid on screen. The Ice Planet is a desolate space, covered in snow and ice. It is a place people come for hard, exploitative labor. We see images of factories and frozen landscapes. We hear the whirring and moaning of the same machines that presumably destroyed Roja’s home planet. Alternatively, the Planet with No Rain is a desert space where Roja seeks healers/healing, while the Ocean Moon is a place of leisure and distraction where people go to escape the rigors of the Ice Planet. In each space, the visuals are supplemented with immersive sound. The Ice Planet is accompanied by a disturbing white noise. We hear machines, engines, perhaps the sound of traffic. The other two planets are characterized by natural sounds, waves crashing, the wind blowing hard against the microphone. In another context, this invasive noise would be a disruptive mistake. Here it reminds us that the natural world always surpasses our attempts to silence her. Some moments have no sound at all, leaving us to our own silence.

Redshift and Portalmetal has several different endings, all of them hopeful. It is designed in Scalar, a platform designed for scholarly publishing. But with a few programming modifications the story comes alive as a dynamic mix of video, ambient sound, and hypertext. The choice of platform is a reinforcement of the worldview conveyed in Redshift. A tool designed according to standards for scholarly publication becomes an engine for change.

Works Cited:
micha cárdenas. “Dilating Destiny: writing the transreal body through game design.” Jump Cut: A Review of Contemporary Media 57 (Fall 2016): n. pag. Jump Cut. Web. 8 June 2017.

Screenshots:


Author statement:
Redshift & Portalmetal asks: as climate change forces us to travel to the stars and build new homes and families, how do we build on this land, where we are settlers, while working to undo colonization? The story uses space travel as a lens through which to understand the experience of migration and settlement for a trans woman of color. Redshift & Portalmetal tells the story of Roja, who's planet's environment is failing, so she has to travel to other worlds. The project takes the form of an online, interactive game, including film, performance and poetry. I designed the interaction, wrote the text, performed the movement, and coordinated the filming in Los Angeles and Toronto. The project is built with HTML5 video, CSS and Javascript, using the Scalar e-publishing platform.

Read the original work online here.

Settled Habits, New Tricks: Casteist Policing Meets Big Tech in India

Ameya Bokil, Avaneendra Khare. Nikita Sonavane, Srujana Bej and Vaishali Janarthanan

STATE OF POWER 2021

May 2021

Big Tech is reinforcing and accelerating a system of caste-based discrimination in India and reinforcing the power and impunity of its police.

It is the evening of 15 June 2019. The Station House Officer of the Kolar Road Police Station in Bhopal, the capital city of the central Indian state of Madhya Pradesh (MP), convenes his officers to announce a rise in car thefts in their jurisdiction. He states that the thieves are the local *Pardhis* and instructs officers to make night-time visits to the *Pardhi basti* (a slum colony), and pick up and detain *anyone* outside after dark. This goes unchallenged because the police widely believe that the *Pardhis* are habitual criminals, responsible for every case of house-breaking and theft. We might have found it hard to believe that the police blatantly target an entire community had we not been at the station for an entirely different reason. Every detained *Pardhi* would have their 'suspicious activity' recorded in the extensive files the police maintain on their community.

Recently, technology companies and governments are helping to digitise these police records and the surveillance of 'suspect' individuals who are more 'likely' to commit crimes. Through this rigged digital database, the Indian police force is being empowered to sustain its caste-based criminalisation of marginalised communities and continue to act arbitrarily with impunity. The digitisation of already biased police records, extensive surveillance systems, predictive policing through interlinked databases and the complete absence of a regulatory framework have led to the creation of a parallel digital caste system which denies the fundamental freedoms of specific marginalised communities.

The Constitution of India formally protects citizens' right to equality, including the right to equal treatment before the law and freedom from discrimination on grounds of race, caste and religion. The adoption of the Constitution was a transformative moment as India became a sovereign, democratic postcolonial republic and aspired to move beyond the pervasive feudal legacy of the caste system. The entrenched nature of the caste system, applying to nearly all aspects of life, has made it hard to extirpate, making the right to equality unattainable for certain communities, as we had witnessed at the police station. The *Pardhi* community is one of India's *Adivasi* or indigenous communities. Although formally outside strictures of the caste system, these communities are nonetheless vilified.

Several hundred communities, including the *Pardhis*, were branded as 'hereditary criminals addicted to systematic commission of non-bailable offences' under the Criminal Tribes Act (CTA) enacted by the British colonial government in 1871. Its aim was to make these communities liable to state surveillance and control in myriad ways. Since the repeal of the CTA in 1952 and the official decriminalisation of the tribes criminalised thereunder, these communities are referred to as De-notified Tribes (DNT).

The CTA was inspired by the combination of racist European criminal anthropology and the Indian caste system, which portrayed criminality as a hereditary characteristic. British colonial authorities established the police in the 1840s with the explicit objective of controlling the Indian population through force. The police failed in in its objective, so to give an appearance of order, it adopted the strategy of selective policing of certain groups. This selection hinged on a social consensus on who was a criminal, informed by the caste system.

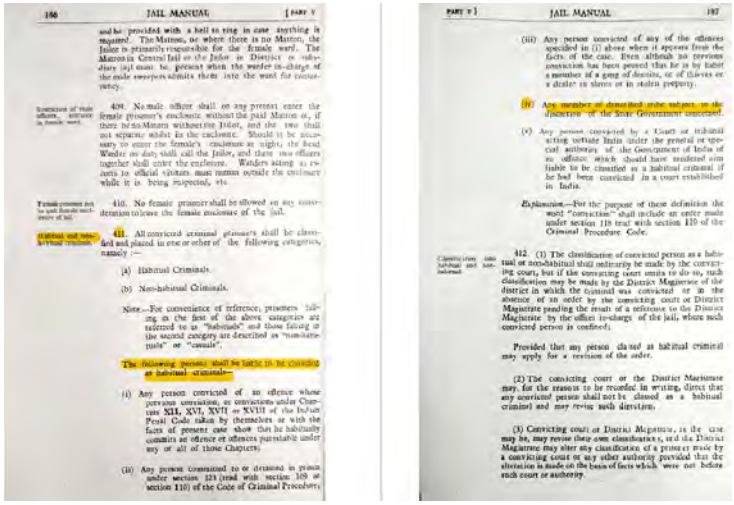
Thus, the colonial strategy created categories of persons who were considered the 'proper objects of policing', principally forest-dwelling and nomadic communities (including *Pardhis*) whose way of life conflicted with British interests. The *Pardhis* are traditionally semi-nomadic hunters, whose way of life conflicted with colonial regulations on hunting, control over forests for commercial purposes and revenue collection from a sedentary population.

Consequently, surveillance and intrusive policing became a part of these communities' daily existence: from having their names registered in permanent records, being placed in 'reformatory settlements' in order to undermine their nomadic cultures and facing severe restrictions on their movement as well as constantly having to report to the authorities. This system is best described by historian Radhika Singha's explanation of the colonial policing system – 'it was far easier to prosecute a prisoner on a charge of

belonging to some ill-defined criminal collectivity than to establish individual responsibility for a specific criminal offence'.

The contemporary Indian police have continued with this legacy. First, Indian society continues to be ordered by the caste system; second, the idea of hereditary criminals still occupies the mind and structure of the Indian police, largely comprising members of oppressive castes; and third on the grounds of expediency that hold as true now as they did during British colonial times.

Thus, limited policing resources are still targeting the same communities. Even after the CTA was repealed, its legacy has endured in policing structures, practices and attitudes. Individual Indian states have adopted legal provisions concerning 'habitual offenders' (HOs) and maintained the surveillance systems designed under the CTA. The hereditary criminal of the past is now placed in the more palatable administrative category of the HO, which remains ill-defined and therefore gives the police vast discretionary powers. These provisions, while apparently neutral, are still selectively used against the same communities that were targeted in colonial times.



References to 'Habitual criminals' in the Madhya Pradesh Jail Manual, 1987, Vol 1, Part 2

'*Angrez chale gaye, police chodh gaye hamare liye*' ('The British are gone, but they have left their police behind'), says a *Pardhi* woman in Bhopal, referring to the continued police discrimination her community faces. Whether in the form of indiscriminate detention, torture in custody, or economic exploitation, the everyday life of *Pardhis* is characterised by police violence; but because they lie at the very bottom of Indian caste society and continue to experience socioeconomic hardship, their systemic exploitation (much like their very existence) is rendered invisible. Scholars have failed to document the systemic police targeting of *Pardhis* and other DNT communities, while civil society's attempts to highlight the issue have been restricted to anecdotal evidence of police brutality.

Once held at a police station, every *Pardhi* – children, women and men – is subjected to physical and verbal assault. 'They know it is easy to beat a confession out of a *Pardhi*', says one woman. Parents are beaten in front of their children to 'send a message.' Recently, two *Pardhi* minors were picked up from a tea-stall and temple, stripped naked and beaten. The police misled their mother about where they were, and when she tried to get them released, she too was beaten by the police and framed under false charges.

Besides the violence, police surveillance has long dispossessed *Pardhis* of their traditional livelihoods. Today, they depend on waste picking, begging and odd jobs like unloading rubble and clearing bushes. 'In the entire city, there is not one person who will offer us employment in a shop or give us any salaried job', claims one *Pardhi*, citing the stigma of criminality associated with DNTs. The constant police surveillance, harassment and frequent arrests hinder their ability to pursue education and steady employment.

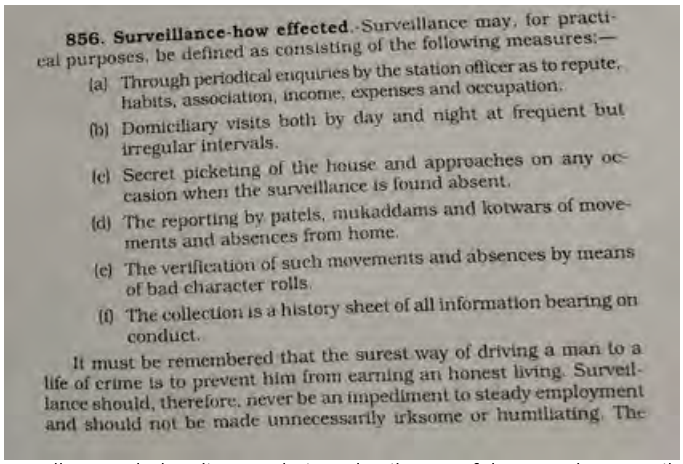
Threatening to create a new police record or add to an existing one, the police demand large bribes (the equivalent of US$ 250–1,500) from the *Pardhi*s. The bribe increases each time they are held in police detention or jailed. Between the bribes, bail and the lack of steady employment, a *Pardhi* family typically remains trapped in a cycle of perpetual indebtedness.

Police stations across India maintain registers of HOs – also called 'history-sheeters' – in their jurisdictions, with extensive details of their lives and daily movements. While their identification may not explicitly be based on caste, collective police action overwhelmingly identifies members of the DNT communities as HOs. These registers record their demographic details such as place of residence and caste, personal information such as age and identifying marks on the body, and 'evidence' of criminality: details of their habits, their method of committing crimes, their property, particulars of their associates, places they frequent, etc.

For communities such as the *Pardhis*, even being visibly mobile carries with it a threat of police surveillance and violence. Rana, a middle-aged *Pardhi* man, was stopped by traffic police for not wearing a crash helmet. When the police demanded to know his surname and caste identity, he was detained and questioned about how he had obtained a motorcycle. When his answers were deemed 'unsatisfactory', he was arrested. So pervasive is the fear of having one's daily life recorded in police registers that Rana, much like other *Pardhis* identified as a HO, rethinks every activity of his life, including something as mundane as going to the local tea stall with friends. These records shackle the *Pardhi* community's lives, freedoms and dignities.

Arguably, the most important section of the habitual offenders' registers is an informal record that police officers must sign to attest that they have personally trailed or surveilled the HO at least once *every* fortnight to investigate whether s/he had (despite extensive surveillance) managed to outwit the police to commit a theft or burglary. The police in Bhopal's Govindpura police station showed us this, which was surprising given that these registers are fiercely guarded to avoid public scrutiny.

State police regulations allow them to maintain a record of HOs in their jurisdictions, but there are no restrictions on the information they can keep in their registers and therefore no form of accountability. As a result, the police have developed their own practices, including using local informants (known as *mukhbirs*) to keep abreast of HOs' daily activities and movements.



856. Surveillance-how effected.-Surveillance may, for practical purposes, be defined as consisting of the following measures:—

(a) Through periodical enquiries by the station officer as to repute, habits, association, income, expenses and occupation.

(b) Domiciliary visits both by day and night at frequent but irregular intervals.

(c) Secret picketing of the house and approaches on any occasion when the surveillance is found absent.

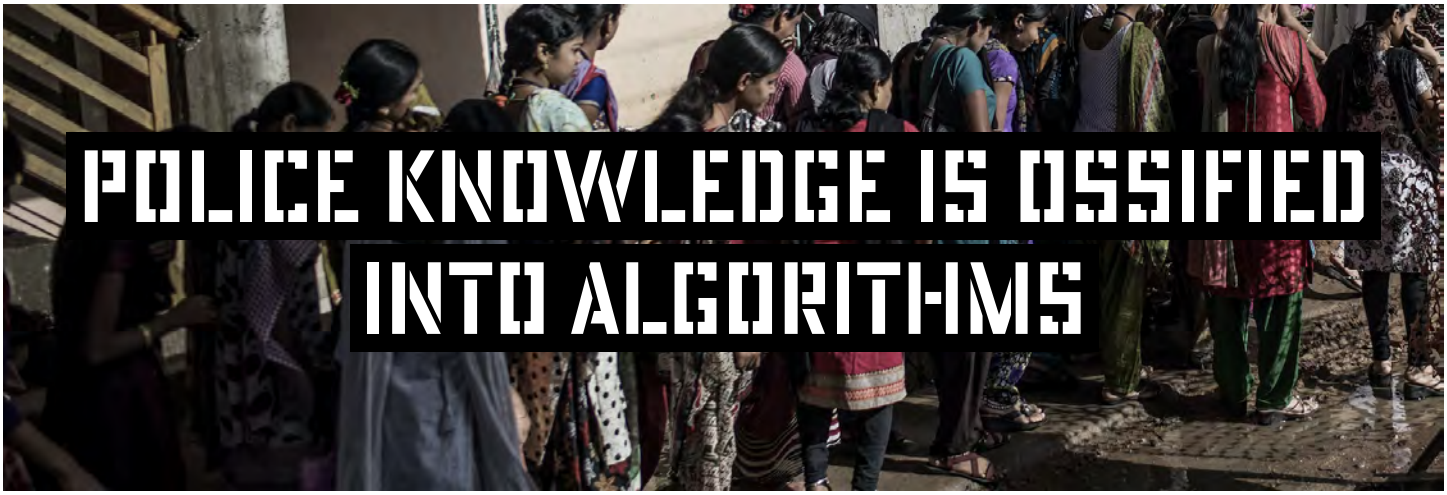
(d) The reporting by patels, mukaddams and kotwars of movements and absences from home.

(e) The verification of such movements and absences by means of bad character rolls.

(f) The collection is a history sheet of all information bearing on conduct.

It must be remembered that the surest way of driving a man to a life of crime is to prevent him from earning an honest living. Surveillance should, therefore, never be an impediment to steady employment and should not be made unnecessarily irksome or humiliating. The

Madhya Pradesh Police Regulations detail some of the ways they surveil suspect individuals and communities



For over a century, the police have kept physical records of all cases and HOs, but these are now being digitised through the Crime and Criminal Tracking Network & Systems (CCTNS), the main and centralised system for maintaining digital records. The central government provides the core infrastructure to standardise digital data: First Information Reports (FIRs), various documents related to investigation and evidence, and the final police reports to be submitted to the courts. The CCTNS also allows geo-tagging of offences. However, for various state governments which are trying to build their own infrastructure over and above this standard, CCTNS extends far beyond digitisation into setting up a crime-mapping, analytics, and a predictive system.

A super platform and an opaque black box, the CCTNS has been designed to be *the* digital repository of every local police record. It is hoped that it will make policing more efficient by allowing local police stations to know about a person's entire criminal history at the click of the mouse: cases in which the person has

been accused, facial photographs, the crimes committed, the number of days held in detention, and whether the courts acquitted or convicted them.

The central government and the tech industry maintain that systems such as the CCTNS will allow for 'objective', 'smart', error-free algorithm-based detection of criminal hotspots and predictive policing. In reality since these databases are fed by the police's centuries-long caste-based system of preventive surveillance and predictive policing (which has already determined who is a criminal and what crimes habitual criminals commit repeatedly), there is no possibility of objectivity or lack of caste bias. The CCTNS only adds a technological veneer to a caste-based policing model. While the ideological purpose matters little to local police stations, its material benefits include hours of saved time and seamless digital transmission of produced criminalities across jurisdictions.

The government and the tech industry maintain that [digital] systems will allow for 'objective', 'smart', algorithm-based detection of criminal hotspots and predictive policing. In reality since these databases are fed by the police's centuries-long caste-based system of preventive surveillance and predictive policing there is no possibility of objectivity or lack of caste bias.

The reliance on and aspirations for predictive policing are a part of the aim for the Indian police to be among the world's most advanced and professionalised force. The police claim that their limitations are inadequate staffing, poor technological skills and an overworked force. The goal is to have the same technological tools in every police station in India as in London and New York, to increase efficiency and technological expertise and obviate the need to recruit more police officers while also cutting workloads. Despite concerns raised about predictive policing in the UK and US with respect to racial profiling and discrimination, mass surveillance, arbitrary search and seizure, as well as the erosion of the fundamental right to privacy, the Indian police have sought to enhance predictive policing technologies such as hotspot detection and data mining.

The CCTNS is the future of India's police registers. By 2030, it is hoped that the platform will be adequately developed to free police officers of maintaining any paper registers. Since state governments are free to tweak CCTNS as they please, several states have been collecting biometric details (iris scans, facial

prints, etc.) of HOs and even first-time offenders. A senior police officer in Bhopal claimed that the CCTNS is being used in Madhya Pradesh as a repository of all criminals. CCTNS integrates various dossiers: history sheets and *goonda* files, fingerprints, footprints, details about family members of accused persons, etc. The details of family members are obtained for a 'deterrent effect', so that purported criminals do not commit further crimes. (A *goonda* is what the police call individuals who are more likely to commit assault or disturb public peace by indulging in general public violence and rioting. Derived from a pejorative term in Hindi that roughly translates as 'rowdy' or 'hooligan', the police surveilled such identified individuals through various *Goonda* Acts from as early as 1926.)

Permanent databases do not spare children either. One 16-year-old *Pardhi* had his details forcibly recorded (including fingerprints and photos) on a charge for which he was eventually given a suspended sentence. Creating permanent records of children, whether or not they are convicted, may be in direct contravention of the Juvenile Justice (Care and Protection of Children) Act, 2015, which espouses the principle of a 'fresh start' for a child. This, however, is of no concern to the local cop.

The problem here, much like in the case of traditional surveillance, is that the police operate without a clear legal framework and use ambiguity to their advantage. The Madhya Pradesh Police Regulations allow for the creation of physical databases of HOs and briefly state the manner of their surveillance. This legal framework, which has remained unchanged over decades, did not foresee today's digital advances. Consequently, using technology for surveillance, with its associated set of new problems (permanence, security, and privacy, to name but a few), has virtually no legal basis and therefore very few constraints. In a landmark judgment in 2017, the Indian judiciary confirmed that Indian citizens have a fundamental right to privacy; however, the judiciary has yet to extend this to the question of maintenance of HO registers and databases.

The only limits to the breadth of police surveillance appear to be infrastructural constraints. To address these problems, the state of Telangana, for instance, is investing in a multi-storey centre to house its ambitious Integrated People Information Hub (IPIH), a database containing 360° profiles of every resident. Other states plan to follow suit.

The state's inability to self-regulate its use of technology is amply demonstrated by the ham-fisted introduction of the Aadhaar, a 'unique identification' number linking biometric

information and various databases necessary for accessing welfare programmes, setting up bank accounts, purchasing SIM cards, and paying income tax, among others until the Supreme Court directed the government to regulate and limit its mandatory use for specific public services.

A second technological advance with regard to policing is the use of closed-circuit cameras (CCTV), purportedly for national security and women's security. A chilling incident of rape and murder that made the headlines in 2012 led to greater calls for harsh criminal laws and mass surveillance technologies to deter crimes against women. The paternalistic preoccupation with maintaining control over women's bodies for the stated purpose of ensuring their safety has resulted in surveillance in public spaces. The Lucknow city police recently announced that they will initiate a response for women in distress based on their facial expressions observed through AI-equipped facial-recognition technology.

Most of the larger Indian cities are dotted with police CCTV (without attendant regulations) on busy streets, at intersections, and in market areas to replace in-person police surveillance. Private establishments and educational institutions in larger cities have also invested in CCTV on their premises in accordance with state regulations seeking to establish 'public safety.' The sinister implications of creating and maintaining such networks are obvious. Recently, during the lockdown imposed to control the COVID-19 pandemic, the Union Government allowed a hate-filled media campaign to vilify Muslims as maliciously spreading outbreaks across India. Unsurprisingly, this culminated in the police in Madhya Pradesh and Telangana using drones to surveil mainly Muslim neighbourhoods.

While CCTV-based surveillance policing has thus far largely maintained the distinction between footage from police cameras and from private cameras mandatorily installed, but accessible only after a crime has been committed, a strange third hybrid is being developed in some parts of the country. Take, for instance, Bhopal Eye, the crown jewel of the Bhopal police surveillance system. This mobile application is marketed as a citizen-policing initiative which allows the police to actively maintain a database of the number, location and range of all private CCTVs installed in the city. As part of the Bhopal Eye initiative, the local police have been 'encouraging' the installation of CCTV in homes and commercial establishments, even in the absence of mandatory public safety regulations.

The economic model of Bhopal Eye, in some ways, parallels mobile applications such as Uber: the financial investment of acquiring and maintaining the input units (CCTVs) for the intended output (surveillance) is made not by the organisation that built the network, but is shifted to citizens by selling to them dual myths of ever-lurking danger and the deterrent value of constant surveillance. When citizens are thus recruited, they can download the free application and log in the location coordinates of their CCTVs. The police, as the database creators, develop this network and use the data to keep track of how many of the city's 'private eyes' can be harnessed for policing purposes. Apart from the lack of *any* regulation, little is known about the procedure used to manage Bhopal Eye, its use and its efficiency. The senior police officer credited with single-handedly constructing and initiating Bhopal Eye declined to answer our questions.

In the future, systems such as Bhopal Eye could, through both overt encouragement and tacit prejudice, facilitate the police's surveillance reach within mixed neighbourhoods, where both affluent and working-class families reside, as well as enable heightened monitoring of 'suspect' individuals, such as street-vendors, in wealthy localities.

Police promotional material shared on social media sites such as Facebook to encourage Bhopal Eye registration with the tagline "No criminal will be safe if houses install cameras properly".

Some members of the DNT communities seem amenable to constant CCTV surveillance. Rana, the man who admitted to being afraid of even going to the local tea stall due to police harassment, exclaims, 'I wish they would actually install CCTVs everywhere so that they would know [that it is not us] who is actually committing these crimes'. The history of CCTV has taught us, however, that the purported safety-net they offer is not for all citizens. For instance, police stations are required to have cameras installed at their entrances and inside cells where the accused are detained. This was supposed to be a check on custodial violence, for which the Indian police are notorious. However, they are now careful to take the accused to a room without CCTV before assaulting them. The police influence medical examinations of the accused to obfuscate the evidence of their brutality. The police hesitate to supply CCTV video feed to those who request it, and the judiciary is not known to strictly demand it either. The reliance on cameras is thus entirely at the discretion of the local police. The police may simply not submit video evidence when it does not favour their case, while the defence might never learn that such evidence exists.

Thus, Rana's trust in the potential benefits of CCTVs seems misplaced. A 2018 incident related to the criminalisation of cattle slaughter in the city of Khandwa illustrates the point. The police had installed CCTVs at a busy town square to check on the illegal slaughter of cattle. A Muslim man, who lived within the range of the surveillance camera, was arrested for the offence. His family repeatedly claimed that the case against him had been fabricated and that the camera's recording would provide the proof needed to exonerate him. However, since the prosecution enjoys wide discretion in introducing evidence at trial, the family had no means of ensuring that the footage made its way to court.

We found almost unreserved enthusiasm for technology in our interviews with the police, with officers at all levels regarding the force's steady progress into increasingly sophisticated methods of data collection and collation as a badge of honour. The only problem, according to the officer in charge of the CCTNS at one of the local police stations, is that the tools currently at their disposal do not work *well enough*. Nor did we have to poke around to find the reasons for this candid embrace since we received the same reply repeatedly: technology makes policing more efficient, convenient, accessible, and accurate – basically, *easier*. Experience suggests that justifications of efficiency need not be set in stone. Be it the precipitous demonetisation implemented in 2016 or the gargantuan *Aadhar* project introduced in 2009, regimes across the political spectrum have displayed a Hydra-like ability to invent and reinvent justificatory strategies, leading one to wonder what exactly lies underneath the screeds and slogans. It is thus meaningful to ask what interests are served by the technological advances but remain obscured from public view.

One need not look far. As Usha Ramanathan, a veteran privacy activist and trenchant critic of the *Aadhaar* project puts unequivocally, 'the driving force behind the [*Aadhaar*] project is corporate interest'. India is a staggeringly lucrative market for private corporations that produce surveillance technologies. In Bhopal, for example, security cameras alone, which are only one component of the city's surveillance infrastructure, cost upwards of Rs. 2.5 Crores (about US $135,000), an enormous figure for a non-metropolitan city.

Indeed, a visit to the futuristic central CCTV control room at the police headquarters in Bhopal is like being at a trade fair, as a support staff member from Honeywell, the corporation behind the city-wide Integrated Video Management System project, rattles off the panoply of brands that have coalesced to create

this panopticon. Honeywell landed the lucrative contract after its impressive performance at surveilling the *Kumbh Mela*, a Hindu pilgrimage held every 12 years, attended by millions. An eight-member team from Honeywell is constantly circulating around Bhopal's police headquarters to provide 'indispensable' technical support.

The nature of Honeywell's partnership with Bhopal police illustrates two significant ways in which private corporate interests cast an ominous shadow over the 'public good': not only do corporations pull the strings; they also invariably set the stage. Consider the case of Huawei, which has been selling 'safe cities' across the world, of which facial-recognition technology is an integral component, altering its pitch to appeal to diverse potential patrons.

Similarly, Honeywell's offering sees public safety as a function of constant, blanket surveillance, whereby everybody is suspect unless observed otherwise – a vision that it then volunteers to execute and helps the law-enforcement agency navigate. Honeywell's role is currently limited to providing the police with CCTV footage when a crime is committed and they request assistance to discover who the criminal is or track where they might have fled. However, for the police and Honeywell, this is only its secondary, instrumental purpose. The inherent purpose of Honeywell's CCTV footage is that it compels public self-discipline and self-surveillance, and therefore reduces crime.

Another case in point is the proliferation of facial-recognition-based AI technologies that are being marketed to police departments across the country as the 'must have' crime-fighting tools. According to reports, the Surat City Police has a picture intelligence unit that relies on Nippon Electrical Company's proprietary NeoFace technology and vehicle number-plate recognition to track persons of interest. During one of our interviews with a police officer, he alluded to the city's population as 'clients.' This language reveals what is not being openly stated, which is that the state is motivated more by being the customers of shiny curios than acting as the custodian of the citizens' civil rights.

The dream of Digital India was sold to the Indian population by the Narendra Modi government soon after being elected in 2014. A key component of this dream is to build an e-governance model. The need to use technology has been furthered through the myth that tech is neutral in the prevention of crime and curbs the problem of human bias, when all that these systems do is essentially digitise the casteist targeting of communities through the nebulous category of HOs. There is scant reflection on what such a digitised caste system implies, who is responsible for designing it and how it reproduces and reifies hierarchies that are inimical to the criminal justice system.

The goal of efficiency makes no attempt to dislodge the traditional principles of policing: who is kept under surveillance and why remain constant across time and space. Technological advances merely sharpen the blade of police discretion and further entrench its operational biases. This is already a departure from the supposed relationship between technology and law enforcement in countries where police body cams are at least expected to correct implicit bias.

Indeed, in the US, there have long been arguments about the attempt to shroud racist systems under the cloak of objectivity. The historian Khalil Muhammad demonstrated how a 'racial data revolution' in the nineteenth century marshaled science and statistics to make a 'disinterested' case for white superiority. The results of the 1890 census showed that African Americans were disproportionately imprisoned, but rather than interpreting this as a symptom of systemic inequities, the data was understood to be 'objective, colour blind, and incontrovertible'. In this way, crime statistics became the foundation upon which the myth of Black inferiority was constructed.

Likewise, the datasets and models used in newer, tech-based systems are not objective representations of reality. The employment of new technologies that reflect and reproduce existing inequities – but that are promoted and perceived as

more objective or progressive than the discriminatory systems of a previous era – often hides, speeds up, and even deepens discrimination, while appearing to be neutral or benevolent.

A spate of new applications allows the police to access and update information from their mobile phones. The more one asks them about the number of databases the police 'maintain' and their regulatory frameworks, the more obvious it is that even the police have been unable to keep up with the mushrooming of private technologies in their operations. It is unknown how many online databases there are, how information is uploaded onto them, the nature and breadth of this information – and what is the ultimate aim of assembling this large archipelago of digital database infrastructures for police surveillance. These multiple applications, software and databases may (for now) exist in silos, even if they regularly cross-pollinate information. However, they are all so close to each other that they can all be easily interlinked to build dossiers of personal information on all citizens and allow more pervasive institutional profiling, which can then be used to justify differential treatment in schooling, employment, housing, etc., particularly for those belonging to marginalised communities who are identified as HOs.

Thus, when the *Pardhi* community says that the police have the entire history of every member of their community, this is no exaggeration. It is clear that the real aim of surveillance and the unchecked powers it gives to the police is to maintain political hegemony and a very strict, hierarchical social order. Thus, surveillance policing allows for the marriage of profit-making corporations and authoritarian regimes. The social control they seek to maintain is, in turn, in accordance with the casteist social control already enforced by police surveillance.

We need to go beyond resisting the introduction and use of surveillance technologies to question, if not overhaul, the very ethos of policing in India, because it has already perpetuated dangerous predictive policing on the bodies of the marginalised even without these technologies. Unfortunately, the Indian state is increasing its excessive reliance on the institutions of policing to respond to various crises. Recently published data, for instance, documents the state's heavy reliance on policing and colonial-era sedition law to quell dissent on issues ranging from Kudankulam Nuclear Power Plant to the Citizenship Amendment Act, 2019. Each new cause opens up new avenues for criminalising and policing marginalised communities.

New justifications for increased police surveillance will keep multiplying as the state seeks to gain a tighter hold over the social order. Each instance of a perceived threat to the 'internal security' of this social order is fertile ground for intensifying surveillance mechanisms, as has been observed most recently in governments' response to citizens' protests. The habitual offender is to the city what the 'anti-national' dissenter is to the country – an inveterate, antisocial element from whom society needs protection.

Activists, lawyers, students, and a cultivated category of urban Naxals are now all beginning to be at the receiving end of this uninhibited state surveillance and records. In February 2021, *The Washington Post* reported that civil rights activist Rona Wilson's laptop had been hacked into for surveilling and planting false documents implicating him as an enemy of the state. While the hacker's identity is unknown, it is reported that the hacker (an individual or organisation) had extensive resources at their disposal. In 2019, it was reported that the Israeli firm NSO Group's spyware tool Pegasus was used to surveil journalists and human-rights defenders. The NSO Group admitted that it sells Pegasus exclusively to governments and law-enforcement agencies.

Surveillance-based policing to address violence against women is the latest addition to the police's range of responsibilities. Although feminist and women's movements, among others, have questioned the failure of criminal law to address violence against women, the questions of caste-based criminality, policing and intersectionality have largely remained absent from this conversation. The caste-based construction of criminality makes women from marginalised communities the most vulnerable. They suffer the greatest violence but receive no

support from the criminal justice system, because its very structures allow the police to perpetrate such violence in the first place.

A parade of women walking from their dorms to various factories sidestepping sewage and construction. Credit: Andrea Bruce / NOOR

Feminist and civil rights movements in India have essentially failed to question the very ethos of casteist policing in the country. *Pardhi* women recount instances of police harassment when they are at work segregating waste. If the police find anything valuable in their waste-collection bag, they are accused of having stolen it and are dragged to the police station. Some women said that their own jewellery and other items are confiscated and recorded as evidence of theft. In two instances where *Pardhi* women had committed suicide because of police harassment, the state relied on such 'criminal antecedents' to portray these women as criminals and grant the police impunity – as if being a criminal justified being a victim of police violence. The instances of violence against *Pardhi* women are rendered invisible through these constructed narratives of criminality, granting the police complete discretion and impunity.

We therefore need to focus our resistance on the very cause of the problem of disproportionate police targeting of marginalised *Adivasi* communities either through technological surveillance or other means: police discretion and impunity. As gatekeepers of the criminal justice system, the police determine who become the subjects of this system. Investing in building police accountability is the first step in tackling the culture of discretion and impunity that has become synonymous with law and order in India.

By underscoring and drawing attention to forms of coded inequality, not only must we challenge the social dimensions of

technology, but also work against the construction of a parallel digital caste system that essentially intensifies the traditional caste system. At present, those whose bodies are subjected to violence by the carceral system are forced to seek justice from the same system. In the US, the Black Lives Matter (BLM) movement has highlighted the dangers of carceral imagination, the racist systems of policing and the need to invest in non-retributive forms of justice.

A major BLM demand is to defund the police who are designed to criminalise Black communities. Lessons from the movement can be adopted to challenge caste-based oppression in India through policing. This would begin by building a discourse of the casteist nature of policing through advocacy, research and community organising, alongside an active investment in cultivating an imagination of a transformative justice, one that is not designed to prosper on the bodies of marginalised communities, whatever their caste – the eradication of which is another, much larger, struggle.

ABOUT THE AUTHOR

Ameya Bokil, Nikita Sonavane and Srujana Bej are young researchers and lawyers working at a nascent criminal justice collective in Bhopal, India called the Criminal Justice and Police Accountability Project (CPAProject). Ameya Bokil is a human rights researcher examining overcriminalisation and police powers, Nikita Sonavane has worked and written extensively on issues of sexual violence, indigenous self governance and anti-discrimination law, **Avaneendra Khare** is an advocate currently based in Bhopal, **Vaishali Janarthanan** is a final year law student and works in organisational capacity building, and Srujana Bej has pursued field based research on the impact of Aadhaar-based biometric authentication on access to socio-economic rights. @srujana_bej @CPAProjectIndia

Photo credit +

State of Power 2021 Credits

« Previous Read | State of Power 2021 | Next Read »

BIG BROTHER IS WATCHING

Chandigarh Govt Is Using Watches to Track Sanitation Workers. We Ask an Expert Why It Violates Their Rights.

By Amlan Sarkar
Aug 4, 2022

SHARE

Image Credit: PTI/Hitesh Sonar For The Swaddle

Last week, the Internet Freedom Foundation in a tweet mentioned that the Chandigarh Municipal Corporation, while responding to a Right To Information (RTI) request, revealed that it had been using tracking watches to keep an eye on sanitation workers since 2020. There are existing reports on workers in Haryana and Rajasthan being subjected to advanced surveillance for assessment of their work. The technology used in these surveillance apparatuses is invasive, dehumanizing, and has left the workers severely disadvantaged.

The Swaddle's Amlan Sarkar spoke to Anushka Jain, Associate Policy Counsel (Surveillance & Transparency) at the Internet Freedom Foundation to better understand the implications of using advanced

surveillance technology on workers, and to explore the nexus of surveillance, labor, and caste.

The Swaddle: Why is the use of surveillance technology to track sanitation workers concerning?

Anushka Jain: It's important to understand that while any employer has the right to assess the quality of the work and whether the work is being done, it cannot be a disproportionate response to the aim that they want to achieve. In a landmark ruling on the Right to Privacy, the Supreme Court of India had said that to justify state intrusion into the privacy of citizens, the state has to make sure that it fulfills certain thresholds — legality, necessity, and proportionality — and it also needs to have procedural safeguards in place to ensure that no misuse happens.

Legality means that there needs to be a law to make sure that there is a framework in which these actions take place — which in this case is missing. A municipal corporation order or any other government authority order saying that they're going to use it (surveillance technology) does not mean that they have provided the action with a legal framework that would provide support to how the use is going to take place, and to ensure that no misuse happens.

Necessity means that the purpose for the invasion of privacy should be a legitimate cause that requires such an invasion. According to the reports that we have been able to access, the aim of these watches — not just in Chandigarh, but also in other places like Nagpur, Lucknow, Noida — is to ensure attendance; that nobody else is doing the work that somebody has been allotted; and that the work is getting done. All of these purposes can be fulfilled in other, much less intrusive manners.

The third threshold — proportionality — says that the intrusion has to be proportionate to the invasion of privacy. For the purpose of attendance and ensuring that work is getting done, imposing these devices on the sanitation workers is a very disproportionate response. They track each and every movement of the workers; they have a camera and a microphone. These features can lead to a very, very serious invasion of privacy, which is not required for the purpose that they want to achieve.

This is why we filed an RTI request, and the response confirmed our suspicion about how this technology is being used and how

disproportionate the use of this technology is.

TS: What are the implications of using surveillance technology on workers?

AJ: When it comes to workplace surveillance, what is necessary to understand is that there is a power equation. Surveillance can lead to opportunities in which the person holding power can misuse the information that they have collected. Any workplace — not just sanitation workers — if surveillance is being conducted, the employee cannot stand up for their rights, because they don't have any legal framework to point to and say, "you are violating this," to employers. In such a situation, the employer can almost do anything that they want, and the employees are totally at their mercy. We're seeing this happen to not just the sanitation workers. A lot of people who work in IT companies or law firms work with extremely invasive software that has been downloaded onto their computers, which is how their employers monitor their work. Screen usage, keyboard strokes — each and every step is being tracked. This level of surveillance can be really harmful to the mental health of a person, and also lead to a violation of freedom of speech. A lot of employees can't voice their opinions about any misgivings with their employer, or any demands that they have with the employer. They can't even discuss it with their co-workers, because they're monitored to the extent that anything that they say or do can reach their superior. We don't want to be at the mercy of good employers; we want to ensure that all employers have to follow certain conditions. And there have to be certain checks and balances that if they don't follow those rules, there is some recourse that is available.

Related on The Swaddle:

Asia Is the World's Surveillance Hotspot, Aiding Authoritarianism in the Covid19 Era: Report

---

TS: Several employers are justifying increased surveillance on their workers as a WHO-mandated step in the wake of the pandemic. Why is this problematic?

AJ: In terms of how different technologies have been used, from the Arogya Setu app, to drones, to any other kind of technology for facial recognition, all add up to a data collection exercise. The government authorities say that they do it for public health, but in the absence of a data protection law or any legislation regulating how this data collection exercise

works, you never know how your information is going to be used after the purpose for which you provide it is fulfilled because there's also no mandate. There's no condition that the government has to delete your data or has to stop using your data. So, once they have collected the data, they can do whatever they want, which is really harmful. For instance, with the Arogya Setu app, we saw that a lot of information — including location data — was collected, and all of this happened for some period of time without any data protection policies. Eventually, they introduced a data protection policy for the app, which has now lapsed. In this situation, again, we are at the mercy of the authorities that are carrying out this exercise to make sure that they don't misuse our data, or that there's no cyber security threat to our data, but there's nothing that protects us or gives us recourse if something bad happens.

TS: Can the implications of excessively surveilling Safai Karamcharis invariably amount to targeting marginalized communities? Who has access to the data and how can it be potentially used against these communities?

AJ: While caste and class are separate categories, they are very deeply intertwined. Sanitation workers especially belong to communities that have been historically discriminated against, which are economically weak, and are weak in the sense of political power. And in such a situation, it's very easy to dehumanize these communities because of the existing caste bias that is there in the country. It's very important to again look at the ways in which power plays out in these categories because it's a person belonging to an upper class or upper caste who is going to surveil somebody belonging to a lower class or lower caste. In such a situation, people who have been historically discriminated against are once again at the mercy of the people who have discriminated against them. Caste definitely has a bearing on the whole situation, because it is still a very important factor not just in rural India, but also in urban India. So, even though Chandigarh is a very urban city, there is no denying that such kind of caste-based discrimination is still taking place there.

TS: And can surveillance worsen the existing caste divide?

AJ: The level of invasion that surveillance technology allows for is unprecedented. The use of these kinds of technologies against people who have already been discriminated against is obviously going to cause even more harm than they have faced historically. For example, the use of CCTVs to surveil certain areas where people belonging to marginalized

communities reside, will lead to an over-policing of these communities — who were already historically over-policed — even more. All of us know that a lot of police brutality happens in India, a lot of people are in jail without trial. These technologies help the police [or the state] track things that might not have been an issue were it to happen in an urban, economically forward area of a city, but would probably lead to an arrest in an area where marginalized people reside. And CCTV is not even an advanced surveillance technology, but its use can lead to a lot of harm. Similarly, the use of any other kind of surveillance technology will also cause disproportionate harm to these communities.

TS: Is worker surveillance a labor rights issue that affects all of us? What are our existing protections against it, if any, and who is protected?

AJ: It's definitely a labor issue. If workers are being surveilled, they can't speak up about any issue they might be facing. One of the ways in which union-busting happens is through surveillance, through tracking each and every movement of people who are trying to unionize and making sure that they don't unionize. So workplace surveillance is certainly a labor rights issue, because it affects how workers are able to wield their other rights. In the absence of privacy, they will not have freedom of speech, they will not have the safety to voice their opinions to their peers. They will not have the ability to raise their demands to their superiors as well, because the superiors might have some information about them, which they might misuse. So it's definitely a labor issue. In terms of protection, we don't have any protection under any law, which relates to privacy, as we don't have a privacy or a data protection law.

TAGS BIG BROTHER IS WATCHING | PRIVACY | SURVEILLANCE

WRITTEN BY AMLAN SARKAR

Amlan Sarkar is a staff writer at TheSwaddle. He writes about the intersection between pop culture and politics. You can reach him on Instagram @amlansarkr.

SEE ALL ARTICLES BY AMLAN

In India, Digital Snooping on Sanitation Workers

Lower-caste cleaners must wear GPS-enabled smartwatches, raising questions about their privacy and data protection.

BY **QADRI INZAMAM & HAZIQ QADRI**

05.02.2022

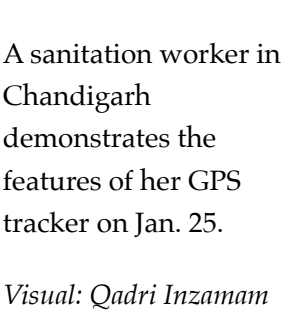
Top: A street sweeper walks on a sidewalk in New Delhi on February 21, 2022. Visual: SAJJAD HUSSAIN/AFP via Getty Images

MUNESH SITS BY the roadside near a crowded market in Chandigarh, a city in India's north, on a January day. She is flanked by several other women, all of them sweepers hired by the Chandigarh Municipal Corporation. She shows the smartwatch she is wearing and says, "See, I didn't even touch it, but the camera has turned on."

Munesh, who estimates she is in her 40s and, like many Indians, goes by just one name, is one of around 4,000 such sanitation workers. The corporation makes it mandatory for them to wear smartwatches — called Human Efficiency Tracking Systems — fitted with GPS trackers. Each one has a microphone, a SIM embedded for calling workers, and a camera, so that the workers can send photos to their supervisors as proof of attendance. In Chandigarh, this project is run by Imtac India, an IT services company, at a cost of an estimated $278,000 per year.

Meanwhile, sanitation workers say that the government has not invested in personal protective gear throughout the Covid-19 pandemic, and that they have long worked without medical care and other vital social services.

From the time the sanitation workers turn on their watches until they turn them off, their GPS locations are monitored in real time by officials at the Command and Control Center of the Chandigarh Municipal Corporation. The workers appear as green dots on a computer screen and as they move around in their assigned areas, the green dot moves along a line.



A sanitation worker in Chandigarh demonstrates the features of her GPS tracker on Jan. 25.

Visual: Qadri Inzamam

The camera fitted on the tracker is what scares Munesh and many other sanitation workers, who mostly come from the Dalit community or other Hindu lower castes. (In the Indian subcontinent, the caste system has long categorized and limited people's education and work prospects; the job of cleaning or sanitation has always been linked to the lower castes.) Wearing the tracker is mandatory. According to Krishan Kumar Chadha, the former president of the Chandigarh Sanitation Workers' Union, taking it off incurs a fine of half a day's salary, around $3 to $4, although Abhay Khare of Imtac India denies there is such a fine. Workers also have to take the

devices home. They worry about privacy leaks and the inability to turn off the trackers and cameras — even when they are in the bathroom.

One of the flagship programs of Indian Prime Minister Narendra Modi is to bring "digital innovations" to the country. Under this Digital India initiative, Modi has been pushing for cashless or digital transactions, digital attendance, and surveillance systems, like the one in place for the sanitation workers. This digital attendance and tracking system is also part of another much-hyped campaign of the government: the Clean India Mission, also known as Swachh Bharat Abhiyan, which launched in October 2014 with the goal of a clean and sanitary India.

These systems come with incentives for the municipalities. Civic bodies with a digital attendance system earn extra points toward an annual list of the country's "cleanest" cities, an honor that gives them bragging rights. This online surveillance of sanitation workers is currently operational in more than a dozen cities, including Indore, Nagpur, Navi Mumbai, Panchkula, Thane, and Mysuru.

The Chandigarh Municipal Corporation introduced GPS-enabled smartwatches for its sanitation workers in 2019. The government says that the tracking devices bring transparency into the attendance system and prevent workers from allowing someone else to sub in for them.

But the workers have been protesting ever since, arguing that the watches violate their privacy and rights. For her part, Munesh says, "it's like an iron shackle around our necks."

N AUGUST 2017, the Supreme Court of India, through a judgment, recognized privacy as a fundamental right.

"Among basic rights conferred on individuals by the Constitution as a shield against excesses by the State, some rights are at the core of human existence," the top court said in its judgment. "Thus, they are granted the status of fundamental, inalienable rights essential to enjoy liberty. Liberty is the freedom of an individual to do what he pleases and the exercise of that freedom would be meaningless in the absence of privacy."

In 2018, a 10-member committee, headed by a retired Supreme Court judge, submitted a comprehensive report on data protection. The committee also suggested a draft data protection bill; a revised version is still pending before a Joint Parliamentary Committee and could be scrapped in favor of new data privacy legislation.

When it comes to surveillance of sanitation workers, "the Constitution does not allow this kind of a thing," says Pavan Duggal, a cyberlaw consultant and advocate for the Supreme Court of India. As such, Duggal argues, the sanitation tracking system violates workers' right to privacy.

> *For her part, Munesh says, "it's like an iron shackle around our necks."*

Although a law passed in 2000 called the Indian Information and Technology Act does allow digital surveillance or interception of citizens under certain circumstances, Duggal adds, the sanitation trackers amount to "crystal clear illegal interception."

A 29-year-old cleaner named Neerjo didn't know that officials at the Command Center can trace the location of her house through the tracker until her interviews with Undark. She was taken aback. "We did not know this," she says and looks at her co-workers in surprise. "We have never been told anything about the watch." Undark repeatedly contacted Chandigarh Municipal Corporation Commissioner Anindita Mitra to verify this and other details about the smartwatch program; the calls and emails went unanswered.

Still, Abhay Khare, business head of Imtac India — a distribution partner of ITI Limited in Chandigarh — insists that the GPS trackers are not breaking laws, and that they follow all the parameters of data safety and privacy. He adds that the devices are also used for government security, "so the ITI Limited is very careful about these parameters."

Before he left his position as project coordinator of Chandigarh's human efficiency tracking system program, Suraj Kumar also told Undark that on the smartwatches, neither the microphone nor the camera can be controlled remotely, which means that no one in the control center can turn them on.

But that does not assuage the fears of the sanitation workers, particularly women. Many say they avoid using the bathroom while on duty. Others put the smartwatches in purses or pockets beforehand — because, says a worker named Mithlesh, "sometimes we go to [the] washroom and the camera turns on automatically, causing problems." Around a dozen women who spoke to Undark shared the same concern.

RELATED

For India's Caste-Based Sewer Cleaners: Robots?

And even though the officials at the CMC stress that the data of sanitation workers are secured and deleted after three months, the workers also complain they often receive spam calls on their smartwatches. "One night, I was awoken by a call on my smartwatch around 11:30 [p.m.]," says one worker, Shakuntala. "I picked it up and some man was asking me who I was. I hung up, knowing it was an unknown number and not someone from my office. How did he get my number if the SIM was given by the Corporation?"

Khare says the GPS trackers do not allow unwanted calls. “It’s impossible they would get spam calls,” he says, adding he had checked it himself.

The workers say the tracking device invades their personal lives. They are required to charge GPS devices at home each night, to make sure the watches remain on during working hours the next day. If the watch is off, the workers are marked absent, risking their wages. According to Chadha of the Chandigarh Sanitation Workers’ Union, the fine for losing the tracker ranges from around $107 to $134, almost their month’s salary.

Taking these devices home aggravates the problems, says Shakuntala. “When I am around the watch, I get conscious,” she adds.

In each part of the city, a supervisor looks after a team of sanitation workers and marks their attendance. A supervisor named Satyapal Singh tells Undark that if a worker’s watch turns off or shows them outside the area where they should be working, even if they are marked present on the register, they don’t get paid.

Pradeep, who drives a sewage truck, says he once got a call from his supervisor, inquiring why he was absent for a week. Although he had been at work, at the Command Center, he was marked inactive. It took Pradeep a few days to prove that he was on duty, he says: “My salary would have been slashed otherwise.”

A **FEW DAYS** before India's Republic Day in January 2022, Chadha, the former president of the Chandigarh Sanitation Workers' Union and a current senior member, sits in his office, a makeshift tin shed, outside a bustling market near the Municipal Corporation office. He sits with workers as they talk about the cleanliness preparation ahead of the special occasion.

But he also stresses the union's presence at an upcoming protest against the tracking devices.

He breaks his conversation with a worker and points towards his smartwatch: "What is this watch?" he asks and leans forward. Then he pauses and sinks in his chair and answers himself, "It is a handcuff that enslaves poor workers." Chadha draws reference from ancient times, saying it is akin to the times when lower castes were physically chained and forced to do menial jobs.

> *"It's modern-day slavery," Wilson said, adding that India's "dominant" castes "still see the sanitation workers as untouchables.*

Khare of IMTAC India boasts of the increased productivity the tracking system has achieved. He says that some local governments using the smartwatches to track field workers have detected employees farming out their work to other people, and that it has been able to save a huge amount of state expenditure.

But the workers complain not only of surveillance, but poor working conditions. At the height of the Covid-19 pandemic, doctors and other health workers in India sometimes faced discrimination and harassment for working with infected patients. But they were also called "frontline warriors" and promised medical insurance. The sanitation workers, who were out on roads, keeping the cities clean, say they have not received adequate personal protection equipment during the pandemic. In a June 2020 independent survey of 214 sanitation workers in several Indian states and metropolitan areas, 56 percent said they weren't given any Covid-19 safety instructions or training. (Twenty-six of those surveyed did not answer this question.)

Even before the Covid-19 pandemic, the sanitation workers say, they were never provided with any safety or protection gear. They also say they are not given any paid leave, medical treatment, or insurance.

Bezwada Wilson, National Convener of Safai Karmachari Andolan — a human rights organization pushing to end manual scavenging,

a traditional practice reserved for Indians from Scheduled Castes — says the surveillance, which he calls illegal, is dehumanizing. It reinforces the idea of slavery, he adds, and stems from the casteist mindset.

"It's modern-day slavery," he said, adding that India's "dominant" castes "still see the sanitation workers as untouchables. As if that was not enough, this tracking device has only reinforced that idea."

Before her lunch break ends, Munesh asks for help with checking how many steps she has walked so far that day. Since her shift started at 7 a.m., her tracker shows she has walked 2,231 steps in the first half of her shift. There are four more hours to go, and one of her coworkers says they cannot afford breaks. Even if they finish their jobs early, they should appear in motion on the screen.

As soon as her lunch break ends, Munesh prepares to leave. She picks up a broom, walks away towards a bustling market, and bends to sweep the litter.

Qadri Inzamam is an independent journalist based out of New Delhi. He writes on the intersections of politics, human rights, and technology.

Haziq Qadri is an independent multimedia journalist based out of New Delhi. His work focuses on the human rights, politics, and health.

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Section No	Title	Page
	CHAPTER 1: PRELIMINARY	
1	Short Title and Commencement	2
2	Definitions	2
3	Interpretation	5
4	Application of the Act	5
	CHAPTER 2: OBLIGATIONS OF DATA FIDUCIARY	
5	Grounds for processing digital personal data	6
6	Notice	6
7	Consent	7
8	Deemed consent	9
9	General obligations of Data Fiduciary	10
10	Additional obligations in relation to processing of personal data of children	12
11	Additional obligations of Significant Data Fiduciary	13
	Chapter 3: RIGHTS & DUTIES OF DATA PRINCIPAL	
12	Right to information about personal data	14
13	Right to correction and erasure of personal data	14
14	Right of grievance redressal	14
15	Right to nominate	15
16	Duties of Data Principal	15
	Chapter 4: SPECIAL PROVISIONS	
17	Transfer of personal data outside India	15
18	Exemptions	16
	Chapter 5: COMPLIANCE FRAMEWORK	
19	Data Protection Board of India	17
20	Functions of the Board	17
21	Process to be followed by the Board to ensure compliance with the provisions of the Act	18

22	**Review and Appeal**	**19**
23	**Alternate Dispute Resolution**	**20**
24	**Voluntary Undertaking**	**20**
25	**Financial Penalty**	**20**
Chapter 6: MISCELLANEOUS		
26	**Power to make Rules**	**21**
27	**Power of Central Government to amend Schedules**	**22**
28	**Removal of difficulties**	**22**
29	**Consistency with other laws**	**22**
30	**Amendments**	**23**
Schedule 1		**24**

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.

Chapter 1: PRELIMINARY

1. Short Title and Commencement

(1) This Act may be called the Digital Personal Data Protection Act, 2022.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint. Different dates may be appointed for different provisions of this Act. Any reference in any provision of this Act to the commencement of this Act shall be construed as a reference to the commencement of that provision.

2. Definitions

In this Act:–

(1) "automated" means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data;

(2) "Board" means the Data Protection Board of India established by the Central Government for the purposes of this Act;

(3) "child" means an individual who has not completed eighteen years of age;

(4) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;

(5) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

(6) "Data Principal" means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child;

(7) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;

(8) "Data Protection Officer" means an individual appointed as such by a Significant Data Fiduciary under the provisions of this Act;

(9) "gain" means-

(a) gain in property or a supply of services, whether temporary or permanent; or

(b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

(10) "harm", in relation to a Data Principal, means -

(a) any bodily harm; or
(b) distortion or theft of identity; or
(c) harassment; or
(d) prevention of lawful gain or causation of significant loss;

(11) "loss" means –

(a) loss in property or interruption in supply of services, whether temporary or permanent; or

(b) a loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

(12) “person” includes—

(a) an individual;
(b) a Hindu Undivided Family;
(c) a company;
(d) a firm;
(e) an association of persons or a body of individuals, whether incorporated or not;
(f) the State; and
(g) every artificial juristic person, not falling within any of the preceding sub-clauses;

(13) “personal data” means any data about an individual who is identifiable by or in relation to such data;

(14) "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

(15) “prescribed” means prescribed by Rules made under the provisions of this Act;

(16) “processing” in relation to personal data means an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(17) “proceeding” means any action taken by the Board under the provisions of this Act;

(18) “public interest” means in the interest of any of the following:
(a) sovereignty and integrity of India;
(b) security of the State;
(c) friendly relations with foreign States;
(d) maintenance of public order;
(e) preventing incitement to the commission of any cognizable offence relating to the preceding sub-clauses; and
(f) preventing dissemination of false statements of fact.

3. Interpretation

In this Act: -

(1) unless the context otherwise requires, a reference to "*provisions of this Act*" shall be read as including a reference to Rules made under this Act.

(2) "*the option to access … in English or any language specified in the Eighth Schedule to the Constitution of India*" shall mean that the Data Principal may select either English or any one of the languages specified in the Eighth Schedule to the Constitution of India;

(3) the pronouns "her" and "she" have been used for an individual, irrespective of gender.

4. Application of the Act

(1) The provisions of this Act shall apply to the processing of digital personal data within the territory of India where:

(a) such personal data is collected from Data Principals online; and

(b) such personal data collected offline, is digitized.

(2) The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.

For the purpose of this sub-section, "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal.

(3) The provisions of this Act shall not apply to:

(a) non-automated processing of personal data;

(b) offline personal data;

(c) personal data processed by an individual for any personal or domestic purpose; and

(d) personal data about an individual that is contained in a record that has been in existence for at least 100 years.

Chapter 2: OBLIGATIONS OF DATA FIDUCIARY

5. Grounds for processing digital personal data

A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act.

For the purpose of this Act, "lawful purpose" means any purpose which is not expressly forbidden by law.

6. Notice

(1) On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data.

(2) Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable.

For the purpose of this section: -

(a) "notice" can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed.

(b) "itemised" means presented as a list of individual items.

***Illustration**: 'A' contacts a bank to open a regular savings account. The bank asks 'A' to furnish photocopies of proof of address and identity for KYC formalities. Before collecting the photocopies, the bank should give notice to 'A' stating that the purpose of obtaining the photocopies is completion of KYC formalities. The notice need not be a separate document. It can be printed on the form used for opening the savings bank account.*

(3) The Data Fiduciary shall give the Data Principal the option to access the information referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution of India.

7. Consent

(1) Consent of the Data Principal means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose.

For the purpose of this sub-section, "specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act.

(2) Any part of consent referred in sub-section (1) which constitutes an infringement of provisions of this Act shall be invalid to the extent of such infringement.

***Illustration**: 'A' enters into a contract with 'B' to provide a service 'X' to 'B'. As part of the contract, 'B' consents to: (a) processing of her personal data by 'A', and (b) waive her right to file a complaint with the Board under the provisions of this Act. Part (b) of the consent by which 'B' has agreed to waive her right shall be considered invalid.*

(3) Every request for consent under the provisions of this Act shall be presented to the Data Principal in a clear and plain language, along with the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act. The Data Fiduciary shall give to the Data Principal the option to access such request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.

(4) Where consent given by the Data Principal is the basis of processing of personal data, the Data Principal shall have the right to withdraw her consent at any time. The consequences of such withdrawal shall be borne by such Data Principal. The withdrawal of consent shall not affect the lawfulness of processing of the personal data based on consent before its withdrawal. The ease of such withdrawal shall be comparable to the ease with which consent may be given.

***Illustration**: 'A' enters into a contract with 'B' to provide a service 'X' to 'B'. As part of the contract, 'B' consents to processing of her personal data by 'A'. If 'B' withdraws her consent to processing of her personal data, 'A' may stop offering the service 'X' to 'B'.*

(5) If a Data Principal withdraws her consent to the processing of personal data under sub-section (4), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing of the personal data of such Data Principal unless such processing without the Data Principal's consent is required or authorised under the provisions of this Act or any other law.

Illustration*: 'A' subscribes to an e-mail and SMS-based sales notification service operated by 'B'. As part of the subscription contract, 'A' shares her personal data including mobile number and e-mail ID with 'B' which shares it further with 'C', a Data Processor for the purpose of sending alerts to 'A' via e-mail and SMS. If 'A' withdraws her consent to processing of her personal data, 'B' shall stop and cause 'C' to stop processing the personal data of 'A'.*

(6) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

For the purpose of this section, a "Consent Manager" is a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

(7) The Consent Manager specified in this section shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal. Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.

(8) The performance of any contract already concluded between a Data Fiduciary and a Data Principal shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

Illustration*: If 'A' enters into a contract with 'B' to provide a service 'X' to 'B' then 'A' shall not deny to provide service 'X' to 'B' on B's refusal to give consent for collection of additional personal data which is not necessary for the purpose of providing service 'X'.*

(9) Where consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by the Data Fiduciary to the Data Principal and consent was given by the Data Principal to the Data Fiduciary in accordance with the provisions of this Act.

8. Deemed consent

A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary:

(1) in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data;

***Illustration**: 'A' shares her name and mobile number with a Data Fiduciary for the purpose of reserving a table at a restaurant. 'A' shall be deemed to have given her consent to the collection of her name and mobile number by the Data Fiduciary for the purpose of confirming the reservation.*

(2) for the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;

***Illustration**: 'A' shares her name, mobile number and bank account number with a government department for direct credit of agricultural income support. 'A' shall be deemed to have given her consent to the processing of her name, mobile number and bank account number for the purpose of credit of fertilizer subsidy amount to her bank account.*

(3) for compliance with any judgment or order issued under any law;

(4) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

(5) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

(6) for taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order;

(7) for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance;

***Illustration**: 'A' shares her biometric data with her employer 'B' for the purpose of marking A's attendance in the biometric attendance system installed at A's workplace. 'A' shall be deemed to have given her consent to the processing of her biometric data for the purpose of verification of her attendance.*

(8) in public interest, including for:

(a) prevention and detection of fraud;

(b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws;

(c) network and information security;

(d) credit scoring;

(e) operation of search engines for processing of publicly available personal data;

(f) processing of publicly available personal data; and

(g) recovery of debt;

(9) for any fair and reasonable purpose as may be prescribed after taking into consideration:

(a) whether the legitimate interests of the Data Fiduciary in processing for that purpose outweigh any adverse effect on the rights of the Data Principal;

(b) any public interest in processing for that purpose; and

(c) the reasonable expectations of the Data Principal having regard to the context of the processing.

9. General obligations of Data Fiduciary

(1) A Data Fiduciary shall, irrespective of any agreement to the contrary, or non-compliance of a Data Principal with her duties specified in this Act, be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf by a Data Processor or another Data Fiduciary.

(2) A Data Fiduciary shall make reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete, if the personal data:

(a) is likely to be used by the Data Fiduciary to make a decision that affects the Data Principal to whom the personal data relates; or

(b) is likely to be disclosed by the Data Fiduciary to another Data Fiduciary.

Illustration*: 'A' has instructed her mobile service provider 'B' to mail physical copies of monthly bills to her postal address. Upon a change in her postal address, 'A' duly informs 'B' of her new postal address and completes necessary KYC formalities. 'B' should ensure that the postal address of 'A' is updated accurately in its records.*

(3) A Data Fiduciary shall implement appropriate technical and organizational measures to ensure effective adherence with the provisions of this Act.

(4) Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach.

(5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed.

For the purpose of this section "affected Data Principal" means any Data Principal to whom any personal data affected by a personal data breach relates.

(6) A Data Fiduciary must cease to retain personal data, or remove the means by which the personal data can be associated with particular Data Principals, as soon as it is reasonable to assume that:

(a) the purpose for which such personal data was collected is no longer being served by its retention; and

(b) retention is no longer necessary for legal or business purposes.

Illustration (A)*: 'A' creates an account on 'X', a Social Media Platform. As part of the process of creating the account, 'A' shares her personal data with 'X'. After three months, 'A' deletes the account. Once 'A' deletes the account, 'X' must stop retaining the personal data of 'A' or remove the means by which the personal data of 'A' can be associated with 'A'.*

Illustration (B)*: 'A' opens a savings account with a bank. As part of KYC formalities, 'A' shares her personal data with the bank. After six months, 'A' closes the savings account with the bank. As per KYC rules, the bank is required to retain personal data for a period beyond six months. In this case, the bank may retain 'A's' personal data for the period prescribed in KYC Rules because such retention is necessary for a legal purpose.*

(7) Every Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the Data Principal's questions about the processing of her personal data.

(8) Every Data Fiduciary shall have in place a procedure and effective mechanism to redress the grievances of Data Principals.

(9) The Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data on its behalf, only under a valid contract. Such Data Processor may, if permitted under its contract with the Data Fiduciary, further engage, appoint, use, or involve another Data Processor in processing personal data only under a valid contract.

10. Additional obligations in relation to processing of personal data of children

(1) The Data Fiduciary shall, before processing any personal data of a child, obtain verifiable parental consent in such manner as may be prescribed.

For the purpose of this section, "parental consent" includes the consent of lawful guardian, where applicable.

(2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause harm to a child, as may be prescribed.

(3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

(4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child for such purposes, as may be prescribed.

11. Additional obligations of Significant Data Fiduciary

(1) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including:

(a) the volume and sensitivity of personal data processed;
(b) risk of harm to the Data Principal;
(c) potential impact on the sovereignty and integrity of India;
(d) risk to electoral democracy;
(e) security of the State;
(f) public order; and
(g) such other factors as it may consider necessary;

(2) The Significant Data Fiduciary shall:

(a) appoint a Data Protection Officer who shall represent the Significant Data Fiduciary under the provisions of this Act and be based in India. The Data Protection Officer shall be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary. The Data Protection officer shall be the point of contact for the grievance redressal mechanism under the provisions of this Act;
(b) appoint an Independent Data Auditor who shall evaluate the compliance of the Significant Data Fiduciary with provisions of this Act; and
(c) undertake such other measures including Data Protection Impact Assessment and periodic audit in relation to the objectives of this Act, as may be prescribed.

For the purpose of this section, "Data Protection Impact Assessment" means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed.

Chapter 3: RIGHTS & DUTIES OF DATA PRINCIPAL

12. Right to information about personal data

The Data Principal shall have the right to obtain from the Data Fiduciary:

(1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;

(2) a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal;

(3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and

(4) any other information as may be prescribed.

13. Right to correction and erasure of personal data

(1) A Data Principal shall have the right to correction and erasure of her personal data, in accordance with the applicable laws and in such manner as may be prescribed.

(2) A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal:

(a) correct a Data Principal's inaccurate or misleading personal data;

(b) complete a Data Principal's incomplete personal data;

(c) update a Data Principal's personal data;

(d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.

14. Right of grievance redressal

(1) A Data Principal shall have the right to readily available means of registering a grievance with a Data Fiduciary.

(2) A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed, may register a complaint with the Board in such manner as may be prescribed.

15. Right to nominate.

A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act.

For the purpose of this section, "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body.

16. Duties of Data Principal.

(1) A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.

(2) A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.

(3) A Data Principal shall, under no circumstances including while applying for any document, service, unique identifier, proof of identity or proof of address, furnish any false particulars or suppress any material information or impersonate another person.

(4) A Data Principal shall furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of this Act.

Chapter 4: SPECIAL PROVISIONS

17. Transfer of personal data outside India

The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.

18. Exemptions.

(1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where:

(a) the processing of personal data is necessary for enforcing any legal right or claim;

(b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function;

(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law;

(d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India.

(2) The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:

(a) by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and

(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board.

(3) The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply.

(4) The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State.

Chapter 5: COMPLIANCE FRAMEWORK

19. Data Protection Board of India

(1) The Central Government shall, by notification, establish, for the purposes of this Act, a Board to be called the Data Protection Board of India. The allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions of the Board shall be digital by design.

(2) The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed.

(3) The chief executive entrusted with the management of the affairs of the Board shall be such individual as the Central Government may appoint and terms and conditions of her service shall be such as the Central Government may determine.

(4) The Board shall have such other officers and employees, with such terms and conditions of appointment and service, as may be prescribed.

(5) The Chairperson, Members, officers and employees of the Board shall be deemed, when acting or purporting to act in pursuance of provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

(6) No suit, prosecution or other legal proceedings shall lie against the Board or its Chairperson, Member, employee or officer for anything which is done or intended to be done in good faith under the provisions of this Act.

20. Functions of the Board

(1) The functions of the Board are:

(a) to determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act; and

(b) to perform such functions as the Central Government may assign to the Board under the provisions of this Act or under any other law by an order published in the Official Gazette.

(2) The Board may, for the discharge of its functions under the provisions of this Act, after giving a person, a reasonable opportunity of being heard and for reasons to be

recorded in writing, issue such directions from time to time as it may consider necessary, to such person, who shall be bound to comply with the same.

(3) The Board may, in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.

(4) The Board may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (2) and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

21. Process to be followed by the Board to ensure compliance with the provisions of the Act

(1) The Board shall function as an independent body and, as far as possible, function as a digital office and employ such techno-legal measures as may be prescribed.

(2) The Board may, on receipt of a complaint made by an affected person or on a reference made to it by the Central Government or a State Government or in compliance with the directions of any court or in case of non-compliance with section 16 of this Act by a Data Principal, take action in accordance with the provisions of this Act.

(3) The Board may authorise conduct of proceedings relating to complaints, by individual Members or groups of Members.

(4) The Board shall first determine whether there are sufficient grounds to proceed with an inquiry. In case the Board determines that there are insufficient grounds, it may, for reasons recorded in writing, close such proceeding.

(5) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act.

(6) The Board shall conduct such inquiry following the principles of natural justice including giving reasonable opportunity of being heard and shall record reasons for its actions during the course of such inquiry.

(7) For the purpose of conduct of inquiry under this section, the Board shall have powers to summon and enforce the attendance of persons, examine them on oath and inspect any data, book, document, register, books of account or any other document.

(8) Inquiry under this section shall be completed at the earliest. The Board or its officers shall not prevent access to any premises or take into custody any equipment or any item that may adversely affect the day-to-day functioning of a person.

(9) The Board may require the services of any police officer or any officer of the Central Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.

(10) During the course of the inquiry if the Board considers it necessary for preventing non-compliance with the provisions of this Act, it may, for reasons to be recorded in writing, issue interim orders after giving the concerned persons a reasonable opportunity of being heard.

(11) On conclusion of the inquiry and after giving the concerned persons a reasonable opportunity of being heard, if the Board determines that non-compliance by a person is not significant, it may, for reasons recorded in writing, close such inquiry. If the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with section 25 of this Act.

(12) At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant.

(13) Every person shall be bound by the orders of the Board. Every order made by the Board shall be enforced by it as if it were a decree made by a Civil Court. For the purpose of this sub-section, the Board shall have all the powers of a Civil Court as provided in the Code of Civil Procedure, 1908.

22. Review and Appeal

(1) The Board may review its order, acting through a group for hearing larger than the group which held proceedings in a matter under section 21, on a representation made to it, or on its own, and for reasons to be recorded in writing, modify, suspend, withdraw or cancel any order issued under the provisions of this Act and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

(2) An appeal against any order of the Board shall lie to the High Court. Every appeal made under this section shall be preferred within a period of sixty days from the date of the order appealed against.

(3) No civil court shall have the jurisdiction to entertain any suit or take any action in respect of any matter under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken under the provisions of this Act.

23. Alternate Dispute Resolution

If the Board is of the opinion that any complaint may more appropriately be resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation by a body or group of persons designated by the Board or such other process as the Board may consider fit.

24. Voluntary Undertaking

(1) The Board may accept a voluntary undertaking in respect of any matter related to compliance with provisions of this Act from any person at any stage.

(2) Such voluntary undertaking may include an undertaking to take specified action within a specified time, an undertaking to refrain from taking specified action, and an undertaking to publicize the voluntary undertaking.

(3) The Board may, after accepting the voluntary undertaking and with the agreement of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking. Acceptance of the voluntary undertaking by the Board shall constitute a bar on proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (4).

(4) Where a person fails to comply with any term of the voluntary undertaking accepted by the Board, the Board may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act.

25. Financial Penalty

(1) If the Board determines on conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crore in each instance.

(2) While determining the amount of a financial penalty to be imposed under sub-section (1), the Board shall have regard to the following matters:

(a) the nature, gravity and duration of the non-compliance;

(b) the type and nature of the personal data affected by the non-compliance;

(c) repetitive nature of the non-compliance;

(d) whether the person, as a result of the non-compliance, has realized a gain or avoided any loss;

(e) whether the person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;

(f) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the provisions of this Act; and

(g) the likely impact of the imposition of the financial penalty on the person.

Chapter 6: MISCELLANEOUS

26. Power to make Rules

(1) The Central Government may, by, notification make Rules consistent with the provisions of this Act to carry out the provisions of this Act.

(2) Every Rule made under the provisions of this Act shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

27. Power of Central Government to amend Schedules

(1) The Central Government may, by notification, amend Schedule 1 to this Act. No such notification shall have the effect of increasing a penalty specified in Schedule 1 to more than double of what was specified in Schedule 1 when this Act was originally enacted.

(2) Any amendment notified under sub-section (1) shall have effect as if enacted in this Act and shall come into force on the date of the notification, unless the notification otherwise directs.

(3) Every amendment made by the Central Government under sub-section (1) shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the amendment or both Houses agree that the amendment should not be made, the amendment shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that amendment.

28. Removal of difficulties

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, before expiry of five years from the date of commencement of this Act, by an order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

29. Consistency with other laws

(1) The provisions of this Act shall be in addition to, and not construed in derogation of the provisions of any other law, and shall be construed as consistent with such law, for the time being in force.

(2) In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

30. Amendments.

(1) The Information Technology Act, 2000 ("IT Act") shall be amended in the following manner:

(a) section 43A of the IT Act shall be omitted;

(b) In section 81 of the IT Act, in the proviso, after the words and figures "the Patents Act, 1970", the words "or the Digital Personal Data Protection Act, 2022" shall be inserted; and

(c) clause (ob) of sub-section (2) of section 87 of IT Act shall be omitted.

(2) Clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 shall be amended in the following manner:

(a) The words "the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information" shall be omitted;

(b) The proviso shall be omitted.

Schedule 1

(See section 25)

Sl. No.	Subject matter of the non-compliance	Penalty
(1)	**(2)**	**(3)**
1	Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (4) of section 9 of this Act	Penalty up to Rs 250 crore
2	Failure to notify the Board and affected Data Principals in the event of a personal data breach, under sub-section (5) of section 9 of this Act	Penalty up to Rs 200 crore
3	Non-fulfilment of additional obligations in relation to Children; under section 10 of this Act	
4	Non-fulfilment of additional obligations of Significant Data Fiduciary; under section 11 of this Act	Penalty up to Rs 150 crore
5	Non-compliance with section 16 of this Act	Penalty up to Rs 10 thousand
6	Non-compliance with provisions of this Act other than those listed in (1) to (5) and any Rule made thereunder	Penalty up to Rs 50 crore

THE INDIAN TELEGRAPH ACT, 1885

No. 13 of 1885

An Act to amend the law relating to Telegraphs in India

WHEREAS it is expedient to amend the law relating to telegraphs in India; It is hereby enacted as follows:-

PART I
PRELIMINARY

1. Short title, local extent and commencement. – (1) This Act may be called the Indian telegraph Act, 1885.

[(2) It extends to the whole of India.]

(3) It shall come into force on the first day of October, 1885.

2. Repeal and savings. [Rep. By the Repealing Act, 1938 (1 of 1938,) sec.2 and Sch.]

3. Definitions. – in this Act, unless there is something repugnant in the subject or context, -

[(1) "telegraph" means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means.

Explanation. – "Radio waves" or "Hertzian waves" means electro-magnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide;]

(2) "telegraph officer" means any person employed either permanently or temporarily in connection with a telegraph established, maintained or worked by [the Central Government] or by a person licensed under this Act;

(3) "message" means any communication sent by telegraph, or given to telegraph officer to be sent by telegraph or to be delivered;

(4) "telegraph line" means a wire or wires used for the purpose of a telegraph, with any casing, coating, tube or pipe enclosing the same, and any appliances and apparatus connected therewith for the purpose of fixing or insulating the same;

(5) "post" means a post, pole, standard, stay, strut or other above ground contrivance for carrying, suspending or supporting a telegraph line;

(6) "telegraph authority" means the Director General of [Posts and Telegraphs], and includes any officer empowered by him to perform all or any of the functions of the telegraph authority under this Act;

(7) "local authority" means any municipal committee, district board, body of port commissioner or other authority legally entitled to, or entrusted by" the Central or any State Government] with, the control, management of any municipal or local fund.

PART II
PRIVILEGES AND POWERS OF THE GOVERNMENT

4. Exclusive privilege in respect of telegraphs, and power to grant licenses.

(1) Within [India], the Central Government shall have exclusive privilege of establishing, maintaining and working telegraphs:

Provided that the Central Government may grant a license, on such conditions and in consideration of such payments as it thinks fit, to any person to establish, maintain or work a telegraph within any part of [India]:

[Provided further that the Central Government may, by rules made under this Act and published in the Official Gazette, permit, subject to such restrictions and conditions as it thinks fit, the establishment, maintenance and working-

(a) of wireless telegraphs on ships within Indian territorial waters [and on aircraft within or above [India], or Indian territorial waters], and

(b) of telegraphs other than wireless telegraphs within any part of [India].

(2) The Central Government may, by notification in the Official Gazette, delegate to the telegraph authority all or any of it its powers under the first proviso to sub-section (1).

The exercise by the telegraph authority of any power so delegated shall be subject to such restrictions and conditions as the Central Government may, by the notification, think fit to impose.]

[**5. Power for Government to take possession of licensed telegraphs and to order interception of messages.** – (1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

6. Power to establish telegraph on land of Railway Company:- Any Railway company, on being required so to do by the Central Government, shall permit the Government to establish and maintain a telegraph upon any part of the lank of the Company, and shall give every reasonable facility for working the same.

[6A. Power to notify rates for transmission of messages to countries outside India – (1) The Central Government may, from time to time, by order, notify the rates at which, and the other conditions and restrictions subject to which messages shall be transmitted to any country outside India.

(2) In notifying the rates under sub-section (1), the Central Government shall have due regard to all or any of the following factors, namely:-

(a) the rates for the time being in force, for transmission of messages, in countries outside India;

(b) the foreign exchange rates for the time being in force;

(c) the rates for the time being in force for transmission of messages within India;

(d) such other relevant factors as the Central Government may think fit in the circumstances of the case.]

7. Power to make rules for the conduct of telegraphs – (1) The Central Government may, from time to time, by notification in the Official Gazette, make rules consistent with this Act for the conduct of all or any telegraphs established, maintained or worked by the Government or by persons licensed under this Act.

(2) Rules under this section may provide for all or any of the following among other matters, that is to say:-

a. the rates at which, and the other conditions and restrictions subject to which, messages shall be transmitted [within India];

b. the precautions to be taken for preventing the improper interception or disclosure of messages;

c. the period for which, and the conditions subject to which, telegrams and other documents belonging to, or being in the custody of, telegraph officers shall be preserved;

d. the fees to be charged for searching for telegrams or other documents in the custody of any telegraph officer;

e. the conditions and restrictions subject to which any telegraph line, appliance of apparatus for telegraphic communication shall be established, maintained, worked, repaired, transferred, shifted, withdrawn or disconnected;

[(ee) the charges in respect of any application for providing any telegraph line, appliance or apparatus;]

f. the charges in respect of –

i) the establishment, maintenance, working, repair, transfer or shifting of any telegraph line, appliance or apparatus;

ii) the services of operators operating such line, appliance or apparatus;

g. the matters in connection with the transition from a system where under rights and obligations relating to the establishment, maintenance, working repair, transfer of shifting of any telegraph line, appliance or

apparatus for telegraphic communication attach by virtue of any agreement to a system where under such rights and obligations attach by virtue of rules made under this section;

h. the time at which, the manner in which, the conditions under which and the persons by whom the rates, charges and fees mentioned in this sub-section shall be paid and the furnishing of security for the payment of such rates, charges and fees;

i. the payment of compensation to the Central Government for any loss incurred in connection with the provision of any telegraph line, appliance or apparatus for the benefit of any person –

a. where the line, appliance or apparatus is, after it has been connected for use, given up by that person before the expiration of the period fixed by these rules, or

b. where the work done for the purpose of providing the line, appliance or apparatus is, before it is connected for use, rendered abortive by some act or omission on the part of that person;

j. the principles according to which and the authority by whom the compensation referred to clause (i) shall be assessed;

[(jj) the qualifications to be possessed and the examinations, if any, to be passed by the persons employed for the establishment, maintenance or working of any telegraph and the fees to be charges for admission to such examinations;] and

k. any other matter for which provision is necessary for the proper and efficient conduct of all or any telegraphs under this act.

(3) When making rules for the conduct of any telegraph established, maintained or worked by any person licensed under this Act, the Central Government may by the rules prescribe fines for any breach of the same:

Provided that the fines so prescribed shall not exceed the following limits, namely:-

i. When the person licensed under this Act is punishable for the breach, one thousand rupees, and in the case of a continuing breach a further fine of two hundred rupees for every day after the first during the whole or any part of which the breach continues.

ii. When a servant of the person so licensed, or any other person, is punishable for the breach, one-fourth of the amounts specified in clause (i).

[(4) Nothing in this section or in any rules made hereunder shall be construed as –

a. precluding the Central Government from entering into an agreement with a person for the establishment, maintenance and working by that Government on terms and conditions specified in the agreement of any telegraph line, appliance or apparatus for the purpose of affording means of telegraphic communication, where having regard to the number of the lines, appliance or apparatus required by that person for telegraphic communication, it is necessary or expedient to enter into such agreement with him, or

b. subjecting the Central Government to any obligation to provide any telegraph line appliance or apparatus for the purpose of affording means of telegraphic communication.

[(5) Every rule made under this section shall be laid as soon as may be after it is made before each House of Parliament while it is in session for a total period of thirty days [which may be comprised in one session or in two or more successive sessions, and it, before the expiry of the session immediately following the session or the successive sessions aforesaid] both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.]]

[**7A. Saving of existing agreements** – Nothing in section 7 shall authorize the making of any rules determining any agreement entered into by the Central Government with any person before the commencement of the Indian Telegraph (Amendment) Act, 1957 (47 of 1957), relating to the establishment, maintenance or working of any telegraph line, appliance or apparatus for telegraphic communication; and all rights and obligations there under relating to such establishment, maintenance or working hall be determined in accordance with the terms and conditions of such agreement.

7B. Arbitration of disputes – (1) Except as otherwise expressly provided in this Act, if any dispute concerning any telegraph line, appliance or apparatus arises between the telegraph authority and the person for whose benefit the line, appliance or apparatus is, or has been provided, the dispute shall be determined by arbitration and shall, for the purposes of such determination, be referred to an arbitrator appointed by the Central Government either specially for the determination of that dispute or generally for the determination of disputes under this section.

(2) The award of the arbitrator appointed under sub-section (1) shall be conclusive between the parties to the dispute and shall not be questioned in any court.]

8. Revocation of licenses – The Central Government may, at any time, revoke any license granted under section 4, on the breach of any of the conditions therein contained, or in default of payment of any consideration payable there under.

9. Government not responsible for loss or damage – The Government shall not be responsible for any loss or damage which may occur in consequence of any telegraph officer failing in his duty with respect to the receipt, transmission or delivery of any message; and no such officer shall be responsible for any such loss or damage, unless he causes the same negligently, maliciously or fraudulently.

PART III
POWER TO PLACE TELEGRAPH LINES AND POSTS

10. Power for telegraph authority to place and maintain telegraph lines and posts – The telegraph authority may, from time to

time, place and maintain a telegraph line under, over, along, or across, and posts in or upon any immovable property:

Provided that –

a. the telegraph authority shall not exercise the powers conferred by this section except for the purposes of a telegraph established or maintained by the [Central Government], or to be so established or maintained;

b. the [Central Government] shall not acquire any right other than that of user only in the property under, over, along, across in or upon which the telegraph authority places any telegraph line or post; and

c. except as hereinafter provided, the telegraph authority shall not exercise those powers in respect of any property vested in or under the control or management of any local authority, without the permission of that authority; and

d. in the exercise of the powers conferred by this section, the telegraph authority shall do as little damage as possible, and, when it has exercised those powers in respect of any property other than that referred to in clause (c), shall pay full compensation to all persons interested for any damage sustained by them by reason of the exercise of those powers.

11. Power to enter on property in order to repair or remove telegraph lines or posts – The telegraph authority may, at any time, for the purpose of examining, repairing, altering or removing any telegraph line or post, enter on the property under, over, along, across, in or upon which the line or post has been placed.

Provisions applicable to property vested in or under the control or management of local authorities

12. Power for local authority to give permission under section 10, clause (c), subject to conditions – Any permission given by a local authority under section 10, clause (c), may be given subject to such reasonable conditions as that authority thinks fit to impose, as to the payment of any expenses to which the authority will necessarily be put in consequence of the exercise of the powers conferred by that section, or as to the time or mode of execution of any work, or as to any other think connected with or relative to any work undertaken by the telegraph authority under those powers.

13. Power for local authority to require removal or alteration of telegraph line or post – When, under the foregoing provisions of this Act, a telegraph line or post has been placed by the telegraph authority under, over, along, across, in or upon any property vested in or under the control or management of a local authority, and the local authority, having regard to circumstances which have arisen since the telegraph line or post was so placed, considers it expedient that it should be removed or that its position should be altered, the local authority may require the telegraph authority t remove it or alter its position, as the case may be.

14. Power to alter position of gas or water pipes or drains – The telegraph authority may, for the purpose of exercising the powers conferred upon it by this Act in respect of any property vested in or under the control or management of a local authority, alter the position there under of any pipe

(not being a main) for the supply of gas or water, or of any drain (not being a main drain):

Provided that –

a. when the telegraph authority desires to alter the position of any such pipe or drain it shall give reasonable notice of its intention to do so, specifying the time at which it will begin to do so, to the local authority, and, when the pipe or drain is not under the control of the local authority, to the person under whose control the pipe or drain is;

b. a local authority or person receiving notice under clause (a) may send a person to superintend the work, and the telegraph authority shall execute the work to the reasonable satisfaction of the person so sent.

15. Disputes between telegraph authority and local authority – (1) If any dispute arises between the telegraph authority and a local authority in consequence of the local authority refusing the permission referred to in section 10, clause (c), or prescribing any condition under section 12, or in consequence of the telegraph authority omitting to comply with a requisition made under section 13, or otherwise in respect of the exercise of the powers conferred by this Act, it shall be determine by such officer as the [Central Government] may appoint either generally or specially in this behalf.

(2) An appeal from the determination of the officer so appointed shall lie to the [Central Government]; and the order of the [Central Government] shall be final.

Provisions applicable to other property

16. Exercise of powers conferred by section 10, and disputes as to compensation, in case of property other than that of a local authority – (1) If the exercise of the powers mentioned in section 10 in respect of property referred to in clause (d) of that section is resisted or obstructed, the District Magistrate may, in his discretion, order that the telegraph authority shall be permitted to exercise them.

(2) If, after the making of an order under sub section (1), any person resists the exercise of those powers, or, having control over the property, does not give all facilities for this being exercised, he shall be deemed to have committed an offence under section 188 of the Indian Penal Code (45 of 1860).

(3) If any dispute arises concerning the sufficiency of the compensation to be paid under section 10, clause (d), it shall, on application for that purpose by either of the disputing parties to the District Judge within whose jurisdiction the property is situate, be determined by him.

(4) If any dispute arises as to the persons entitled to receive compensation, or as to the proportions in which the persons interested are entitled to share in it, the telegraph authority may pay into the Court of the District Judge such amount as he deems sufficient or, where all the disputing parties have in writing admitted the amount tendered to be sufficient or the amount has been determined under sub-section (3), that amount; and the District Judge, after giving notice to the parties and hearing such of them as desire to be heard, shall determine the persons entitled to receive the compensation or, as the

case may be, the proportions in which the persons interested are entitled to share in it.

(5) Every determination of a dispute by a District Judge under sub-section (3) or sub-section (4) shall be final:

Provided that nothing in this sub-section shall affect the right of any person to recover by suit the whole or any part of any compensation paid by the telegraph authority, from the person who has received the same.

17. Removal or alteration of telegraph line or post on property other than that of a local authority – (1) When, under the foregoing provisions of this Act, a telegraph line or post has been placed by the telegraph authority under, over, along, across, in or upon any property, not being property vested in or under the control or management of a local authority, and any person entitled to do so desires to deal with that property in such a manner as to render it necessary or convenient that the telegraph line or post should be removed to another part thereof or to a higher or lower level or altered in form, he may require the telegraph authority to remove or alter the line or post accordingly:

Provided that, if compensation has been paid under section 10, clause (d) he shall, when making the requisition, tender to the telegraph authority the amount requisite to defray the expense of the removal or alteration, or half of the amount paid as compensation, whichever may be the smaller sum.

(2) If the telegraph authority omits to comply with the requisition, the person making it may apply to the District Magistrate within whose jurisdiction the property is situated to order the removal or alteration.

(3) A District Magistrate receiving an application under sub-section (2) may, in his discretion reject the same or make an order, absolutely or subject to conditions, for the removal of the telegraph line post to any other part of the property or to higher or lower level or for the alteration of its form; and the order so made shall be final.,

Provisions applicable to all property

18.Removal of trees interrupting telegraphic communication – (1) If any tree standing or lying near a telegraph line interrupts, or is likely to interrupt, telegraphic communication, a Magistrate of the first or second class may, on the application of the telegraph authority, cause the tree to be removed or dealt with in such other way as he deems fit.

(2) When disposing of an application under sub-section (1), the Magistrate shall, in the case of any tree in existence before the telegraph line was placed, award to the persons interested in the tree such compensation as he thinks reasonable, and the shall be final.

19. Telegraph lines and posts placed before passing of this Act.- Every telegraph line or post placed before the passing of this Act under, over, along, across, in or upon any property, for the purposes of a telegraph established or maintained by the [Central Government], shall be deemed to have been placed in exercise of the powers conferred by, and after observance of all the requirement of, this Act.

[**19 A. Person exercising legal right likely to damage telegraph or interfere with telegraphic communication to give notice –** (1) Any person desiring to deal in the legal exercise of a right with any property in such a manner as is likely to cause damage to a telegraph line or post which has been duly placed in accordance with the provisions of this Act, or to interrupt or interfere with telegraphic communication, shall give not less than

one month's notice in writing of the intended exercise of such right to the telegraph authority, or to any telegraph officer whom the telegraph authority may empower in the behalf.

(2) If any such person without having complied with he provisions of sub-section (1) deals with any property in such a manner as is likely to cause damage to any telegraph line or post, or to interrupt or interfere with telegraphic communication, a Magistrate of the first or second class may, on the application of the telegraph authority, order such person to abstain from dealing with such property in such manner for a period not exceeding one month from the date of his order and forthwith to take such action with regard to such property as may be in the opinion of the Magistrate necessary to remedy or prevent such damage, interruption or interference during such period.

(3) A person dealing with any property in the manner referred to in sub-section (1) with the bona fide intention of averting imminent danger of personal injury to himself or any other human being shall be deemed to have complied with the provisions of the said sub-section if he gives such notice of the intended exercise of the right as is in the circumstances possible, or where no such previous notice can be given without incurring the imminent danger referred to above, if he forth with gives notice of the actual exercise of such right to the authority of officer specified in the said sub-section.

19B. Power to confer upon licensee powers of telegraph authority under this Part – The Central Government may, by notification in the Official Gazette, confer upon any licensee under section 4, in respect of the extent of his license and subject to any conditions and restrictions which the Central Government may think fit to impose and to the provisions of this Part, all or any of the powers which the telegraph authority possesses under this Part with regard to a telegraph established or maintained by the Government or to be so established or maintained:

Provided that the notice prescribed in section 19A shall always be given to the telegraph authority or officer empowered to received notice under section 19A(1).

PART IV
PENALTIES

[**20. Establishing, maintaining or working unauthorized telegraph –** (1) If any person establishes, maintains or works a telegraph within [India] in contravention of the provisions of section 4 or otherwise than as permitted by rules made under that section, he shall be punished, if the telegraph is a wireless telegraph, with imprisonment which may extend to three years, or with fine, or with both, and in any other case, with a fine which may extend to one thousand rupees.

(2) Not withstanding anything contained in the Code of Criminal Procedure, 1898 (5 of 1898), offences under this section in respect of a wireless telegraph shall, for the purposes of the said Code, be bailable and non-cognizable.

(3) When any person is convicted of an offence punishable under this section, the Court before which he is convicted may direct that the telegraph in respect of which the offence has been committed, or any part of such telegraph, be forfeited to Government.]

[**20A. Breach of condition of license –** If the holder of a license granted under section 4 contravenes any condition contained in his license, he shall be punished with fine which may extend o one thousand rupees, and with a further fine which may extend to five hundred rupees for every week during which the breach of the condition continues.]

21. Using unauthorized telegraphs – If any person, knowing or having reason to believe that a telegraph has been established or is maintained or worked in contravention of this Act, transmits or receives any message by such telegraph, or performs any service incidental thereto, or delivers any message for transmission by such telegraph or accepts delivery of any message sent thereby, he shall be punished with fine which may extend to fifty rupees.

22. Opposing establishment of telegraphs on railway land – If a Railway Company, or an officer of a Railway Company, neglects or refuses to comply with the provisions of section 6, it or he shall be punished with fine which may extend to one thousand rupees for every day during which the neglect or refusal continues.

23. Intrusion into signal-room, trespass in telegraph office or obstruction – If any person –

a. without permission of competent authority, enters the signal-room of a telegraph office of the Government, or of a person licensed under this Act, or

b. enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or

c. refuses to quit such room or enclosure on being requested to do so by any officer or servant employed therein, or

d. willfully obstructs or impedes any such officer or servant in the performance of his duty,

he shall be punished with fine which may extend to five hundred rupees.

24. Unlawfully attempting to learning the contents of messages – If any person does any of the acts mentioned in section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under section 23) be punished with imprisonment for a term which may extend to one year.

25. Intentionally damaging or tampering with telegraphs – If any person, intending –

a) to prevent or obstruct the transmission or delivery of any message, or

b) to intercept or to acquaint himself with the contents of any message, or

c) to commit mischief,

damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof,

he shall be punished with imprisonment for a term which may extend to three years, or with fine or with both.

[25A. Injury to or interference with a telegraph line or post – If, in any case not provided for by section 25, any person deals with any property and

thereby willfully or negligently damages any telegraph line or post duly placed on such property in accordance with the provisions of this Act, he shall be liable to pay the telegraph authority such expenses (if any) as may be incurred in making good such damage, and shall also, if the telegraphic communication is by reason of the damage so caused interrupted, be punishable with a fine which may extend to one thousand rupees:

Provided that the provisions of this section shall not apply where such damage or interruption is caused by a person dealing with any property in the legal exercise of a right if he has complied with the provisions of section 19A (1).]

26. Telegraph officer or other official making away with or altering, or unlawfully intercepting or disclosing, messages, or divulging purport of signals – If any telegraph officer, or any person, not being a telegraph officer but having official duties connected with any office which is used as a telegraph office.

a. willfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or

b. willfully, and otherwise than in obedience to an order of the Central Government or of a State Government, or of an officer specially authorized [by the Central or a State Government] to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent Court, discloses the contents or any part the contents of any message, to any person not entitled to receive the same, or

c. divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same,

he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

27. Telegraph officer fraudulently sending messages without payment – If any telegraph officer transmits by telegraph any message on which the charge prescribed by the [Central Government], or by a person licensed under this Act, as the case may be, has not been paid, intending thereby to defraud the [Central Government], or that person, he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

28. Misconduct – If any telegraph officer, or any person not being a telegraph officer but having official duties connected with any office which is used as a telegraph office is guilty of any at of drunkenness, carelessness of other misconduct whereby the correct transmission or the delivery of any message is impeded or delayed or if telegraph officer loiters or delays in the transmission or delivery of any message, he shall be punished with imprisonment for a term which may extend to three months, or with fine which may extend to one hundred rupees, or with both.

29. [Sending fabricated messages] Rep. By the Indian Telegraph (Amendment) Act, 1971 (33 of 1971), sec 4.

[29A. Penalty – If any person, without due authority, -

a. makes or issues any document of a nature reasonably calculated to cause it to be believed that the document has been issued by, or under the authority of, the Director-General of [Posts and Telegraphs], or

b. makes on any document any mark in imitation of, or similar to, or purporting to be, any stamp or mark of any Telegraph Office under the Director General of [Posts and Telegraph], or a mark of a nature reasonably calculated to cause it to be believed that the documents so marked has been issued by, or under authority of, the Director-General of [Posts and Telegraphs],

he shall be punished with fine which may extend to fifty rupees.]

30. Retaining a message delivered by mistake – If any person fraudulently retains, or willfully secretes, makes away with or detains a message which ought to have been delivered to some other person, or, being required by a telegraph officer to deliver up any such message, neglects of refuses to do so, he shall be punished with imprisonment for a term which may extend to two years, or with fine, or with both.

31. Bribery – A telegraph officer shall be deemed a public servant within the meaning of sections 161, 162, 163, 164 and 165 of the Indian Penal Code (45 of 1860); and in the definition of "legal remuneration" contained in the said section 161, the word "Government" shall, for the purposes of this Act, be deemed to include a person licensed under this Act.

32. Attempts to commit offences – Whoever attempts to commit any offence punishable under this Act shall be punished with the punishment herein provided for the offence.

PART V
SUPPLEMENTAL PROVISION

33. Power to employ additional police in places where mischief to telegraphs is repeatedly committed – (1) Whenever it appears to the State Government that any act causing or likely to cause wrongful damage to any telegraph is repeatedly and maliciously committed in any place, and that the employment of an additional police force in that place is thereby rendered necessary, the State Government may send such additional police force as it thinks fit to the place, and employ the same therein so long as, in the opinion of that Government, the necessity of doing so continues.

(2). The inhabitants of the place shall be charged with the cost of the additional police force, and the District Magistrate shall, subject to the orders of the State Government, assess the proportion in which the cost shall be paid by the inhabitants according to his judgment of their respective means.

(3). All moneys payable under sub-section (2) shall be recoverable either under the warrant of a Magistrate by distress and sale of the movable property of the defaulter within the local limits of his jurisdiction, or by suit in any competent Court.

(4). The State government may, by order in writing, define the limits of any place for the purposes of this section.

[34A. Application of Act to Presidency-towns – (1) This Act, in its application to the Presidency-towns, shall be read as if for the words "District Magistrate" in section 16, sub-section (1), and section 17, sub-sections (2) and (3), for the words "Magistrate of the first or second class" in section 18, sub-section (1), [and section 19A, sub-section (2),] and for the word "Magistrate" in section 18 sub-section (2), there had been enacted the words

"Commissioner of Police", and for the "District Judge" in section 16, sub-sections (3), (4) and (5), the words "Chief Judge of the Court of Small Causes".

(2) Omitted.

(3) The fee in respect of an application to the Chief Judge of a Presidency Court of Small Causes under sub-section (3) of section 16 shall be the same as would be payable under the Court-fees Act, 1870 (7 of 1870), in respect of such an application to a District Judge beyond the limits of a Presidency-town, and fees for summonses and other processes in proceedings before the Chief Judge under sub-section (3) or sub-section (4) of that section shall be payable according scale set forth in the Fourth Schedule to the Presidency Small Cause Courts Act, 1882.

35. Reference to certain laws of Part B States. [Rep. by Part B States (Laws) Act 1951 (Act 3 of 1951), sec.3 and Sch.]

****

The Indian Telegraph (Amendment) Act, 2003

THE INDIAN TELEGRAPH (AMENDMENT) ACT, 2003

No. 8 OF 2004

[*9th January*, 2004.]

An Act further to amend the Indian Telegraph Act, 1885.

BE it enacted by Parliament in the Fifty-fourth Year of the Republic of India as follows:—

1. (*1*) This Act may be called the Indian Telegraph (Amendment) Act, 2003.

(*2*) It shall be deemed to have come into force on the 1st day of April, 2002.

13 of 1885.

2. In section 3 of the Indian Telegraph Act, 1885 (hereinafter referred to as the principal Act), clause (*1*) shall be renumbered as clause (*1AA*) and before clause (*1AA*) as so renumbered, the following clauses shall be inserted, namely:—

'(*1*) "Fund" means the Universal Service Obligation Fund established under sub-section (*1*) of section 9A;

(*1A*) "Universal Service Obligation" means the obligation to provide access to basic telegraph services to people in the rural and remote areas at affordable and reasonable prices;'.

Amendment of section 4.

3. In section 4 of the principal Act, in sub-section (*1*), the following *Explanation* shall be inserted at the end, namely:—

"*Explanation.*—The payments made for the grant of a licence under this sub-section shall include such sum attributable to the Universal Service Obligation as may be determined by the Central Government after considering the recommendation made in this behalf by the Telecom Regulatory Authority of India established under sub-section (*1*) of section 3 of the Telecom Regulatory Authority of India Act, 1997.". 24 of 1997.

Amendment of section 7.

4. In section 7 of the principal Act, in sub-section (*2*), after clause (*ee*), the following clauses shall be inserted, namely:—

"(*eea*) the manner in which the Fund may be administered;

(*eeb*) the criteria based on which sums may be released.".

Insertion of new Part IIA.

5. After Part II of the principal Act, the following Part shall be inserted, namely:—

"PART IIA

UNIVERSAL SERVICE OBLIGATION FUND

Establishment of Universal Service Obligation Fund.

9A. (*1*) On and from the commencement of the Indian Telegraph (Amendment) Act, 2003, there shall be deemed to have been established, for the purposes of this Act, a Fund to be called the Universal Service Obligation Fund.

(*2*) The Fund shall be under the control of the Central Government and there shall be credited thereto—

(*a*) any sums of money paid under section 9B;

(*b*) any grants and loans made by the Central Government under section 9C.

(*3*) The balance to the credit of the Fund shall not lapse at the end of the financial year.

Crediting of sums to Consolidated Fund of India.

9B. The sums of money received towards the Universal Service Obligation under section 4 shall first be credited to the Consolidated Fund of India, and the Central Government may, if Parliament by appropriation made by law in this behalf so provides, credit such proceeds to the Fund from time to time for being utilised exclusively for meeting the Universal Service Obligation.

Grants and loans by Central Government.

9C. The Central Government may, after due appropriation made by Parliament by law in this behalf, credit by way of grants and loans such sums of money as that Government may consider necessary in the Fund.

Administration and utilisation of Fund.

9D. (*1*) The Central Government shall have the power to administer the Fund in such manner as may be prescribed by rules made under this Act.

(*2*) The Fund shall be utilised exclusively for meeting the Universal Service Obligation.

(*3*) The Central Government shall be responsible for the co-ordination and ensuring timely utilisation and release of sums in accordance with the criteria as may be prescribed by rules made under this Act.".

Repeal and saving.

6. (*1*) The Indian Telegraph (Amendment) Ordinance, 2003, is hereby repealed. Ord. 7 of 2003

(*2*) Notwithstanding the repeal of the Indian Telegraph (Amendment) Ordinance, 2003, anything done or action taken under the principal Act as amended by the said Ordinance, shall be deemed to have been done or taken under the principal Act, as amended by this Act. Ord. 7 of 2003

T. K. VISWANATHAN

SURVEILLANCE (HTTPS://MODELVIEWCULTURE.COM/ISSUES/SURVEILLANCE)

Everyone Watches, Nobody Sees: How Black Women Disrupt Surveillance Theory

Our picture of surveillance needs to factor in not just tech developments, but the cultural standards that have bred surveillance, especially towards black culture, as part and parcel in our world.

—*by* **Sydette Harry (https://modelviewculture.com/authors/sydette-harry)** *on* **October 6th, 2014**

> What the hell is you looking for? Can't a young man get money anymore?

It kind of pains me to call Mason Betha prophetic, but 17 years ago when "Looking at Me" hit the Billboard charts, the Harlem native pretty much described the current state of surveillance and tech in America. Especially for black people and doubly so for black women.

Surveillance is based on a presumption of entitlement to access, by right or by force. More importantly, it hinges on the belief that those surveilled will not be able to reject surveillance — either due to the consequences of resisting, or the stealth of the observance. They either won't say no, or they can't.

Discussions of stolen celebrity selfies often miss the "by force" aspect of the breeches, instead focusing on salacious details. Surveillance is part of the information age, but it has always been part of abusive dynamics. As opting into surveillance becomes increasingly mandatory to participate in societies and platforms, surveillance has been woven into the fabric of our lives in ways we can not readily reject.

Being watched is not just an activity of Big Brother-style surveillance, but also fannish adulation and social enmeshment. As Black women have been historically denied the ability to consent to surveillance, modern discussion of watching and observing black women needs better historical context. When I'nasah Crockett points out how black women online (http://modelviewculture.com/pieces/raving-amazons-antiblackness-and-misogynoir-in-social-media) have constantly been portrayed as "raving amazons," one of the unspoken through lines is how easily media, even on the left, believes dissecting black women, tracking their online habits, consuming illegally obtained images of them, and demanding education is a "right". Black women cannot say no, and do not need to be in any way respected or fully informed about how they will be studied or used. Media collects the data of black activity and media production as a weapon, without black participation. The lack of black participation

can be unintentional or intentional, but usually ends in gross appropriation, clumsy "admiration", willful erasure or a troublesome combo of all three. Combined with historical blindness, racist condescension and content desperation, the modern surveillance of black women too often results in the same historical abuse and erasure of black women.

When Patricia Garcia (http://www.vogue.com/1342927/booty-in-pop-culture-jennifer-lopez-iggy-azalea/) says the that the big booty era has finally arrived as a "high fashion" moment, but credits Jennifer Lopez and Iggy Azaelea, it erases the very real abuse that black bodies have suffered for those exact body types, that were surveilled to produce the standard that Garcia hands over to Lopez et. al. She writes:

> "Rihanna shows up to the CFDA Awards practically naked with her crack fully on display and walks off with a Fashion Icon Award. Perhaps we have Jennifer Lopez to thank (or blame?) for sparking the booty movement."

Suggesting the way to Rihanna's 2014 moment was paved by Lopez shows a dangerous laziness towards the stated goal of body positivity. Rihanna's moment was a direct tribute to Josephine Baker, another black woman often sexualized and placed under surveillance, not just for celebration of her uniquely black body but for her participation in World War II and the civil rights movement. Garcia's "cultural surveillance" ends up being a contextless mess that insults both Rihanna and Baker.

(https://twitter.com/rihanna/status/473952039169310721)

Writing for Salon (http://www.salon.com/2013/12/05/the_american_media_has_no_idea_how_to_talk_about_race_on_s I pointed out that Media has no idea how to talk about race, and more recently I am convinced they do not actually care to learn. Unfortunately when covering Black women, this inability or unwillingness to learn defaults to common stereotypes at best and complete cultural propaganda at worst. That unwillingness create a vacuum of knowledge, as history repeats itself over and over.

Take Alessandra Stanley's profile of Shonda Rhimes in the New York Times: a cringe-worthy attempt at "complimenting" Rhimes' stereotype-breaking television output that instead relies on empty surveillance of black characters while Stanley offers no evidence of having actually watched the shows she cites. Stanley's descriptions of Rhimes and her work are filled with words like "angry, terrorizing and sassy," recalling Crockett's angry amazons perfectly while perpetuating and prolonging logic that for decades kept Viola Davis from being the leading lady (http://www.nytimes.com/2014/09/14/magazine/viola-davis.html?src=me&_r=0) Stanley describes. Her piece ignores multi-year plot developments as well as a wonderful opportunity to discuss Rhimes' accomplishments as possibly the only non-white-male with multiple, simultaneous network TV hits. Her surveillance provides little in the way of edification and a lot in codifying uncomfortable catch 22's for black women and privacy: visibility is part of achievement in media, but is it worth it when *even at the pinnacle of your success* the only thing made visible is the racism of those observing you?

Even more difficult, how do you fight back?

Photo CC-BY Disney/ABC Television Group, filtered.
(https://www.flickr.com/photos/disneyabc/14180784084/)

Under Surveillance, Over Exposed

Steven Mann's concept of sousveillance centers on wearing portable cameras and technology to record activity, but I would like to expand it to include all forms of using tech to jam surveillance. Mann, a pioneer in the field of wearable computing and computation photography, framed the concept of wearable cameras functioning as recording data for the *user,* not an outside network. Hashtags, street recordings, phone taps can all be looked at as ways of using tech to push back against surveillance. #Yourslipisshowing in particular was used to fight #4chan surveillance of black women. Crockett, user @sassycrass, and a community of black women (myself included) used the hashtag to expose 4chan board members who declared "war" on black feminists by tracking and attempting to infiltrate their "ranks." The attempt was foiled mostly by how their racist caricatures of black women (much like Stanley's) were so jarringly incongruent with reality.

However, sousveillance often requires large amounts of disclosure to be effective and ultimately negates privacy even more. Hasan M. Elahi responded to being incorrectly (http://archive.wired.com/techbiz/people/magazine/15-06/ps_transparency)surveilled by making a project of displaying his personal information (http://elahi.umd.edu/track/). Similarly, Black women's responses to abusive surveillance has often been heart-rending accounts of personal trauma and exposure of personal networks. What goes unmentioned is that social capital and safety are often key to being able to go public with sousveillance as a strategy. Mann and Elahi – credentialed, well-known professors – have a much easier time of saying they agree to be watched than those on the margins.

Stacia L. Brown (http://www.washingtonpost.com/news/act-four/wp/2014/09/11/how-the-fashion-media-erase-black-women/) offers a beautiful examination of the ramifications of ahistorical surveillance, discussing representation as well as more diverse media sources as counter-tactics. As Brown points out in response to Garcia's flippant mess: "It isn't about who gets credit for popularizing the 'big booty.' It's about who is erased and minimized in the process."

Her recommendations are solid but also bring up a very real question: for populations whose fundamental problem under surveillance is the inability to declare privacy and boundaries, what kind of solution is being made to expose one's self "voluntarily," to invite more observation into one's life?

The response to these articles and continued moments of ahistorical abuse and sometimes outright violence are a version of cultural sousveillance. Black women must lay themselves bare, exposing trauma and constantly excavating painful historical memory to gain sympathy and respect. Surveillance must be used as sousveillance, with the records generated by the intrusive observation of blackness, used to bolster black testimony.

Buzzfeed has an article that is a triggering reminder (http://www.buzzfeed.com/jtes/daniel-holtzclaw-alleged-sexual-assault-oklahoma-city#3ztyni1) of the murkiness of this dilemma. While being one of the few places to acknowledge how Daniel Holtzclaw, a predatory policemen targeted black women, it also notes how he used surveillance, and even the more stringent sousveillance to track black women to abuse. To emphasize the gravity of his offense, once again black women's trauma is made public with overly specific details on the abuse of his victims.

More disturbingly have been the deaths of three black men: Eric Garner, Michael Brown and John Crawford III, all murdered by police. In all three cases there was video /photo evidence of the deaths that circulated the internet, and in Brown's case, even AFTER the mother requested it stop. Crawford's death is a disturbing illustration of the interplay of surveillance and sousveillance with historical discrimination. The police who ultimately ended his life were responding to a report, via citizen surveillance, that he had been observed with a gun. The surveillance video which showed him being shot? Still not enough for indictment.

Why must black death be broadcast and consumed to be believe, and what is it beyond spectacle if it cannot be used to obtain justice (http://www.npr.org/blogs/thetwo-way/2014/09/25/351422552/grand-jury-wont-indict-officers-in-ohio-wal-mart-shooting)?

History Repeating

Photo CC-BY ibkod, filtered. (https://www.flickr.com/photos/ibkod/4186747311/)

When Janay Rice was assaulted by her husband, it became a rallying cry for domestic violence and resulted in job creation for white feminists. What stuck out immediately was the ease at which the surveillance aspects were skipped over. Echoing a similar leak of a private moment that targeted the Knowles-Carter family, little discussion was made of how a culture of intrusion seemed to focus on the abuse of black women as breaking news without asking about breaches of boundaries.

That the same online communities that continually prodded and mocked black women are incubators for sex criminals who expose private pictures of celebrities isn't shocking, it's inevitable. They watched the world not care, why should they anticipate consequences now? Predators are often wrongly pictured as targeting the defenseless, when they also target the undefended. Black people, women particularly have historically been able to defend themselves, but have also been shown to be undefended. The problem is not that they *can't* fight back, but that their fight and the record of what they were fighting is erased and sanitized for easier consumption.

When Laurie Penny and Lola Okolosie (http://www.theguardian.com/commentisfree/2014/jun/18/sexist-racist-online-sabotage-wont-win-posing-online-feminists-leftists) claim a victory over racist and sexists online, they willfully erase the original problem of targeted women not wanting to be surveilled, and shut down conversations about how that issue can be addressed. If they have won already, what does the trauma of the women used in that success matter?

Just recently, threats to "expose" Emma Watson's nudes turned out to be a prank to "draw attention (http://mashable.com/2014/09/24/emma-watson-nude-leak-viral-marketing/)" to attacks on feminists. The very real trauma of women — who even after they were transgressed were asked to answer for it like they had committed the crime — becomes a "gotcha" moment. A time to ask what factors lead to the abuse of women and where it starts — usually

with black women expressing feminist or anti-racist ideals — becomes covered in really uncomfortable racist/classist overtones, namely: "What happens if this happens to a white woman we actually care about?!" Even as women of all colors have been fighting for years to make legislation against revenge porn.

When Janay Rice was assaulted by her husband, it became a rallying cry for domestic violence and resulted in job creation for white feminists (http://espn.go.com/nfl/story/_/id/11531293/roger-goodell-nfl-create-social-responsibility-role-help-domestic-violence-social-issues). It's a cry that does not truly encompass the necessary complexity (https://sports.vice.com/article/the-nfls-domestic-violence-problem-and-our-race-problem) of the problem in the NFL, or give anything at all to the attacked woman. This major step to "address issues" still hinges on making a black woman's personal affairs heartbreakingly public and assuring that no one who represents her voice — which has asked for very different things than advocacy — will be heard.

What We Call Surveillance

Photo CC-BY Andy Roberts, filtered. (https://www.flickr.com/photos/aroberts/3035796/)

What we have decided to call surveillance is actually a constant interplay of various forms of monitoring that have existed and focused on black people, and specifically black women, long before cameras were around, let alone ubiquitous. Surveillance technology is a dissemination of cultural standards of monitoring. Our picture of surveillance needs to factor in not just tech developments, but the cultural standards that have bred surveillance, especially towards black culture, as part and parcel in our world.

Elahi can use the intrusion into his privacy to further his work. But if all you want to do is have space to mind your own business, handle your family issues in private, or exist without interference, sousveillance isn't an answer... it's a reminder of defeat. If what you want is representation *as you are,* what do you do when the reality is ignored for the easy win, even when it leaves you worse than before?

What is the solution for being constantly watched, if no one sees you at all?

consent (https://modelviewculture.com/pieces/tag/consent)

domestic violence (https://modelviewculture.com/pieces/tag/domestic-violence)

history (https://modelviewculture.com/pieces/tag/history)

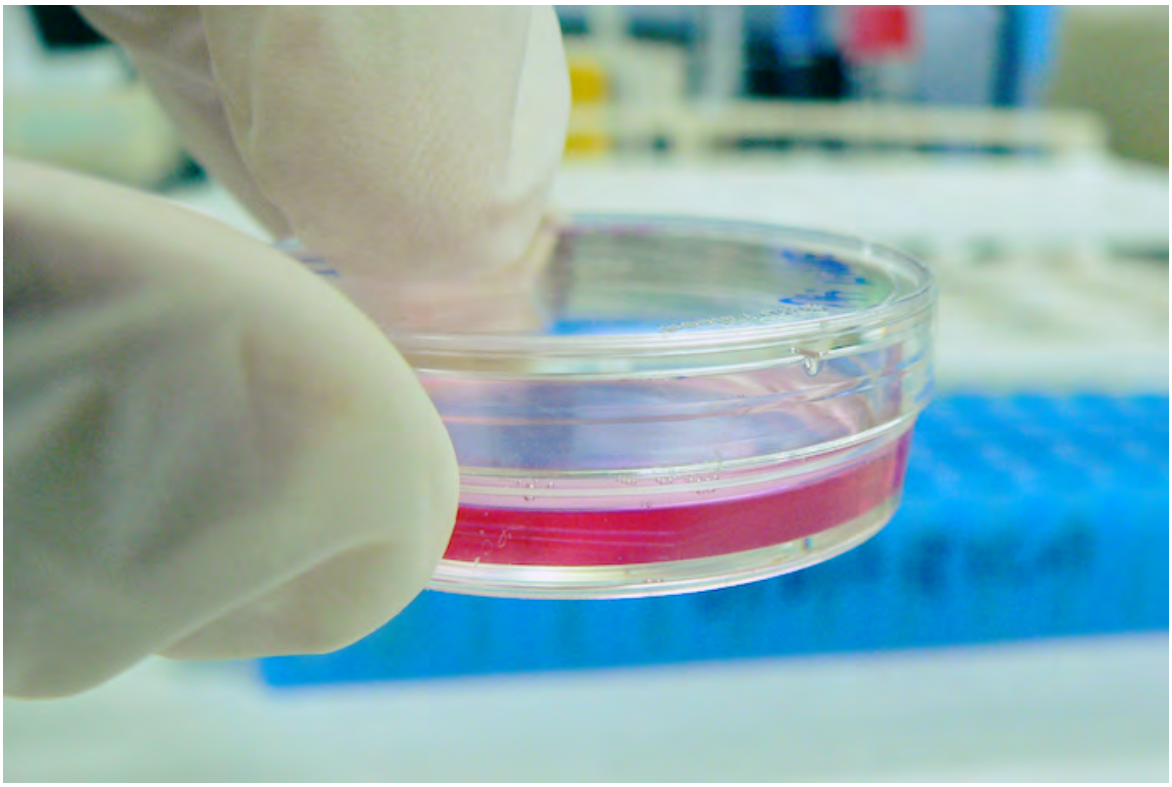
media (https://modelviewculture.com/pieces/tag/media)

race (https://modelviewculture.com/pieces/tag/race)

social media (https://modelviewculture.com/pieces/tag/social-media)

surveillance (https://modelviewculture.com/pieces/tag/surveillance)

violence against women (https://modelviewculture.com/pieces/tag/violence-against-women)



(https://modelviewculture.com/pieces/social-media-and-academic-surveillance-the-ethics-of-digital-bodies)

Social Media and Academic Surveillance: The Ethics of Digital Bodies (https://modelviewculture.com/pieces/social-media-and-academic-surveillance-the-ethics-of-digital-bodies)

— *by* **Dorothy Kim (https://modelviewculture.com/authors/dorothy-kim)**

(https://modelviewculture.com/pieces/grooming-students-for-a-lifetime-of-surveillance)

Grooming Students for A Lifetime of Surveillance (https://modelviewculture.com/pieces/grooming-students-for-a-lifetime-of-surveillance)

— *by* **Jessy Irwin (https://modelviewculture.com/authors/jessy-irwin)**

(https://modelviewculture.com/pieces/big-brother-is-an-asshole)

Big Brother is An Asshole (https://modelviewculture.com/pieces/big-brother-is-an-asshole)

— *by* **Ailsa Sachdev (https://modelviewculture.com/authors/ailsa-sachdev)**

14

Watching the Watchers – What We Can Do to Resist

Knowledge of the depth and extent of the potential dangers facing our society often leaves people feeling understandably dazed and powerless. But the story is not one of unremitting gloom.

Sousveillance and public opinion

To some degree, surveillance cuts both ways. Thanks to the prevalence of video and phone cameras, ordinary citizens now have a means of 'watching the watchers' and recording their observations, an activity known as 'sousveillance' (literally 'watching from below'). Although many 'sousveillance events' are little more than self-indulgent stunts (World Sousveillance Day appears to have involved nothing more provocative than taking still photographs of CCTV cameras), other activists have had major impacts on society. Sousveillance does offer the possibility of logging at least some of the corrupt or illegal practices of the authorities and their agents in such detail that there is no opportunity for 'plausible deniability'.

Perhaps the first effective example of watching the watcher occurred on 3 March 1991 when George Holliday filmed four officers of the LAPD mercilessly beating a lone black man,

Rodney King. King was on parole for a robbery conviction at the time, had failed to stop the car he was driving and had jumped several red lights and stop signs before he was pulled over. The police claimed that King had tried to resist arrest and continued to resist even while being hit with batons. However, the video showed King immobile on the ground and the police continuing to belabour his inert body regardless. The incident became something of a *cause célèbre* and was a major factor in the LA riots a year later. During the ensuing trial only one of the policemen was found guilty, partly because a segment of the video (not widely shown by the media) showed King getting up and attacking a policeman.

More recently, in November 2006, widely-viewed footage on YouTube revealed a UCLA police officer assaulting a student in the university library. The important point here is not merely the act of sousveillance, but the publicising of examples of abuse to the widest possible audience. For example, in August 2007 three police officers of the Sûreté du Québec (Quebec Police) infiltrated a demonstration against the leaders of Canada, Mexico, and the United States at a meeting of the Security and Prosperity Partnership (SPP) in Montebello, Quebec. The demonstrators claimed that the officers were *agents provocateurs*, there to provoke an incident that would discredit the demonstration and allow the deployment of riot police. When the head of the Quebec police denied the allegations and publicly stated that there had been no police presence, a sousveillance video screened on YouTube revealed that he was lying. He quickly revised his statement to say that while police might have been placed among the protestors, they were there as peaceful observers only. Scrutiny of the sousveillance video showed them to be masked, wearing police boots, with at least one holding a rock. At one point Dave Coles, president of the Communications, Energy and Paperworkers Union, had to order the three masked

police 'observers' away from a confrontation with the line of riot police.

The practice of sousveillance has now spread to the developing world. Organisations such as 'Witness' in the USA lend video equipment to human rights activists around the globe, and have led to exposés such as Operation Fine Girl, detailing rape as a weapon of war in Sierra Leone.[1]

But despite such advantages, the balance of power remains vastly in favour of the Big Boys, whose technological reach and firepower will always vastly outweigh that of the individual or action group. Regulation in the form of 'codes of practice' is regularly ignored; legal restrictions are flouted, or made obsolete by rapidly changing technology. Those attempting to implement the global surveillance strategy can only be defeated by a groundswell of public opinion, and by privacy activists willing to fight a long, sustained campaign to raise public awareness. There are parallels here to the eco-warriors of the 70s – dismissed for decades as 'idealistic greenies', they refused to buy into the 'resistance is futile' or 'this is progress' mantras that are promoted so consistently and so effectively by both government and major corporations. Many commentators felt that their goals, though laudable, were idealistic and unrealistic. Yet the eco-warriors persisted, and today much of their agenda is now accepted as mainstream.

Australia provides a perfect, and timely, example of the need for public awareness and the power of public opinion. In 1986 the Australian government signalled its intention of issuing a national identity card (the Australia Card Bill, or ACB). The rationale behind the move was the usual mix of catching benefit frauds and apprehending illegal immigrants, with the added implication that 'only those with something to hide had something to fear'. Most Australians were quickly sold on the idea, with opinion polls showing an 80 per cent approval of the proposal.

Then, slowly at first, but with increasing insistence, questions began to be asked on civil liberties and privacy. When the public heard that the number of government departments intending to require the ID card had leaped from three to 30 their suspicions grew, and were confirmed by the minutiae of the Bill, which listed a host of restrictive penalties. Cardless persons could not be hired or paid (fine for doing so: A$20,000), would be denied access to pre-existing bank accounts, could not cash in investments, give or receive money from a solicitor, or receive funds from unit trusts. They could not buy or rent their own home. If your card was destroyed and you could not prove that its loss was accidental there was a $5,000 fine or two years in prison (or both). Failure to produce your ID on demand at a tax office incurred a A$20,000 penalty. Cardless sick and unemployed people, pensioners, widows and invalids would be denied benefits.

Nor was this likely to be the limit of the repressive measures envisioned for the people of Australia. Aware of possible resistance, the card's architect, the Health Insurance Commission, suggested a plan which discussed the incremental stealth strategy used in so many surveillance proposals with surprising honesty:

> One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially, with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

A parliamentary joint select committee found against the card, pointing out the serious civil liberties implications and warning of a fundamental change in the relationship between citizen and state. Newspapers on the right and left raised their voice against the Bill and many famous Australians joined the clamour. Public opinion, now fully informed, swung solidly against the

ID card and within a few weeks the 80 per cent approval had metamorphosed into an astonishing 90 per cent opposition to the Bill. Faced with a protest of monumental proportions, the government backed down.

It would be nice to report that the victory was permanent. Unfortunately, Thomas Jefferson's old adage on freedom[2] applies with a vengeance to surveillance. While the Australian public quickly lost interest in the ID card issue, their rulers simply bided their time. Two decades later the concept reappeared, when former Australian Prime Minister John Howard announced a scheme (national card; linked to a massive central database; essential to stop fraud and benefit cheats etc) that looked suspiciously like the old ID card idea. But Mr Howard insisted that the two concepts were poles apart and engaged in some outrageous doublespeak to prove it. Just as the UK ID card had become an Entitlement Card, so now the Australian ID was metamorphosed by the magic of political sophistry into the all-new Access Card. Nor was the card to be mandatory for all Australians. 'It will not be compulsory to have the card,' Howard told journalists, adding however that 'it will be necessary for everybody who needs a card to apply for one.' As, from 2010, the provision of health and social services will be denied anyone without an Access Card, then except for those guaranteed lifelong health and prosperity, the card is essential to all Australians. Surprisingly, the scam seems to have worked; the lessons of the 80s have been lost, and a step-wise, stealthy approach has lulled a continent's population into acceptance. This is all the more surprising when other, less intrusive methods of establishing identity are now available.

Designing out surveillance: the privacy card

The UK administration, along with many Western governments, continues to insist on the necessity of ID cards linked to massive databases. These databases, and their interconnectivity, are responsible for a huge number of privacy and civil liberty concerns, not least of which is dataveillance. But as much as the UK government might wish it, there is simply no need for biometric patterns on ID cards, e-passports and the like to be checked against a central database. The pattern can be stored within the smart card itself, with the comparison exercise being performed within the card – which would then say simply 'Yes' or 'No' to the system. In the case of e-passports with fingerprint biometrics, the owner of the passport would place their digit against a fingerprint reader which would then capture the data and convert it to a transitory biometric template. The machine would then electronically interrogate the e-passport and determine if the pattern it had just recorded was the same as the pattern held on the passport. If the patterns matched, identity would be confirmed – and all without resort to any central database.

We can have secure identity without recourse to centralisation. Indeed, there are no technological barriers to the production of a comprehensive 'privacy card' which would act as a buffer to prevent information being centralised. Such a card could disguise the identity of its owner and scramble personal information so as to prevent the collection of sensitive data in large databases by large organisations.

Of course, such cards would still depend upon RFID technology to be effective, leaving the owner vulnerable to a scanning attack by illicit card readers, and a consequent risk of ID theft if the encryption protecting the data is broken (not

to mention the location and surveillance dangers of the technology). Unless we forgo RFID entirely there does not seem to be any way of avoiding such threats. But rejecting RFID passports is by no means a bad idea – other more secure methods of checking and verifying such documents already exist.

Ingenia Technology have developed 'Laser Surface Authentication' (LSA) which allows any document, including a passport or ID card, to be positively identified by virtue of its unique individual surface qualities.[3] When paper or plastic laminate is made, each sheet 'sets' in a one-off configuration dependent on a variety of factors such as fibre orientation, temperature and humidity. The surface of each sheet is as unique as a human fingerprint – it is impossible to counterfeit. The newly-developed Ingenia technology can scan any document to reveal this 'LSA fingerprint' of its surface properties. The system dispenses with any data chip; it is 'read-only' and, once scanned, a record of the document's surface features is stored on a database along with non-biometric details of its owner. When the document is rescanned the appropriate details – name, address, etc, of the owner – can be instantly displayed.

This is a highly accurate system, which not only makes false matching unlikely but allows counterfeit passports to be detected immediately (those documents lacking a database presence would be invalid), and can even detect whether a photograph or name has been altered.

The Royal Academy of Engineering has pointed out that LSA scanning is far more secure than the government-favoured RFID solution. In addition, the Academy's report points out that it 'could also offer privacy gains, as the amount of information on the database available to the person scanning a passport can be controlled – it could be limited to just a name or a photo or even just the assurance that the passport is a genuine passport issued by the appropriate country. This technology could

be used for ID cards. Instead of ID cards having chips on them or information printed on their surface, they could be linked to databases in the same way. Provided the database is secure, then individuals' privacy and security is protected. Alternatively, more advanced privacy schemes are possible where the LSA fingerprint is used as an encryption key for locally held personal information. Traditional technologies such as 2D barcodes can be used to carry the information on the card itself. This offers the same immutability of data as would occur if it was held on a central database, combined with the inability to make identical copies.'[4]

Instead of using such advances that could easily circumvent the known vulnerabilities of RFID-based cards, the UK government (and now the European Union) seems hell-bent on deploying one of the few systems *which absolutely require* the establishment of huge central databases. The question is, of course, why? And the next, *cui bono*? It is most definitely not the citizen. Bureaucracy and big business are the only winners here.

LSA scanning is just one of a number of privacy-enhancing technologies (PETs) which essentially act as countermeasures against the PITs (privacy invasive technologies). The web can be surfed anonymously via sites such as Turbohide.com; web 'cookies' can be filtered; encryption of personal data can prevent corporations (though not governments) from obtaining data; network design and software code can produce a marked regulatory effect;[5] privacy preference tools and smart agents can likewise help to keep the surveillance society at bay. But most countermeasures are for the computer aficionado – those lacking knowledge, awareness or even the wherewithal to implement the available PETs will always remain in the majority.

Some forms of electronic communication, such as email, are still possible anonymously via 'remailers' and other arrangements, who manage a succession of intermediary-operated

services in which (like cells in a resistance or espionage organisation) each intermediary knows only the identity of those adjacent to it in the chain. 'Pseudonymity' is also possible, where substantial protections are put in place, but can be removed under defined legal circumstances. While 'anonymity' sites raise questions of what purpose they may ultimately serve (criminal and terrorist organisations will find them particularly useful), 'pseudonymity' has its own problems, in that the power to override protections is normally in the hands of government or corporations and, as Roger Clarke has commented, 'governments throughout history have shown themselves to be untrustworthy when their interests are too seriously threatened; and corporations are dedicated to shareholder value alone ...'[6]

Privacy Impact Assessment

The similarities between the environmental protests of the 1970s and today's anti-surveillance activism point up a method to slow down or stop the deployment of harmful surveillance systems. With our 'greener' perceptions, the Environmental Impact Assessment (EIA) is now accepted practice throughout the developed world whenever new building or infrastructure developments are mooted. An EIA allows for a review, in advance of any building work, of any possible environmental effects that may accrue from the proposed project. Recently, there have been demands that a similar Privacy Impact Assessment (PIA) be required before the rollout of new surveillance procedures. This call has been heeded in some countries, and both the USA and Canada have mandated the technique for all federal-level, public-sector projects where personal data is processed. So far the UK government has shown interest in the idea, but without moving to any mandatory requirement. This is unfortunate, as

at present new information systems and methods of processing and transferring data between and across departments are often established with little or no regard for privacy concerns. When things go wrong, operators are faced with the challenge of mending the system, often with costly 'bolt-on' solutions that compromise efficiency. Or, as often as not, the problem is simply ignored. A report for the information commissioner by the Surveillance Studies Network explained that, in simple terms, a PIA may be seen as:

- 'an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.'[7]

- 'a process. The fact of going through this process and examining the options will bring forth a host of alternatives which may not otherwise have been considered.'[8]

- an approach and a philosophy that holds promise by instilling a more effective culture of understanding and practice within organisations that process personal data.

- a form of risk assessment, which therefore cannot escape the uncertainties of identifying and estimating the severity and likelihood of the various risks that may appear to privacy, life chances, discrimination, equality and so on.

- a tool for opening up the proposed technologies or applications to in-depth scrutiny, debate and precautionary action within the organisation(s) involved.

- like PETs, premised on the view that it is better to build safeguards in than to bolt them on.

- an early-warning technique for decision-makers and operators of systems that process personal information, enabling them to understand and resolve conflicts between their aims and practices, and the required protection of privacy as set out above or the control of surveillance.

- Ideally, a public document leading to gains in transparency and in the elevation of public awareness of surveillance issues and dangers may be realised; in turn, it may assist regulatory bodies in carrying out their work effectively.

PIAs are long overdue in the United Kingdom, but they are not the whole story. As we have seen, surveillance encompasses more than simple privacy concerns. The time is ripe for an expansion of the PIA concept to one of Surveillance Impact Assessment (SIA), allowing for a review which would encompass the totality of surveillance effects, both individual and societal.[9] As the Surveillance Studies Network report states:

> What an ICT innovation, a new database, or a new audio-visual scheme for monitoring public places or private shopping precincts implies for personal autonomy and dignity, social solidarity, or the texture of social interactions, is not an inconceivable line of enquiry that could become institutionalised as a set of practices and requirements before those surveillance possibilities are implemented.[10]

Despite it being merely common sense and natural justice to ask such basic questions, such a Surveillance Impact Assessment

requirement would demand a painful shift of worldview for government, corporations, and privacy regulators alike. But it is a change they must make if we are to support and maintain such basic values as trust, goodwill and a belief in the democratic process within our increasingly fractured society.

Direct action

If all else fails, it is still possible to organise effective protests against some of the worst excesses of the surveillance society. It is surprising how much surveillance actually depends upon the cooperation or acquiescence of the individual under observation or from whom data is required. The UK government's own figures – made public grudgingly, after three years' delay – reveal that 30 per cent of the UK population is predicted to refuse to cooperate with ID card checks. Should this figure rise to over 50 per cent (as may well occur when the full impact of the ID legislation becomes apparent), the whole scheme could well become unworkable. In addition, workers in the surveillance business may have philosophical issues about the use to which the data they collect is put; they can quite easily disrupt or modify this data collection, degrading its value.

Using cash and postal mail services serves to disconnect you, to some degree, from the surveillance web. Refusing store cards of any colour prevents further entries under your name on marketing lists; obtaining cards in false names further confuses the marketers (anti-surveillance advocate and former MIT professor Gary Marx has obtained store cards in the names of both Karl and Groucho Marx). In a similar way, forms and documents that demand an overabundance of personal details may be filled out with imaginary information. Small errors in

the spelling of names, addresses and other details will create multiple entries in the databases and make successful data-matching less likely. Workers who key in information from forms can similarly introduce deliberate mistakes, and even greater disruption is possible from computer programmers erasing databases (and backups), or introducing logic bombs, Trojan horses and similar disruptive programmes. As Brian Martin has pointed out, a simple magnet can corrupt computer disks. It is even possible to make your own RFID 'fryer' to frustrate clothing tags and ID cards alike, although this practice is fraught with risk and should be discouraged.

Unfortunately, such methods have serious limitations: they may have nuisance value but, given the size and complexity of the surveillance web, they are little more than pinpricks in the hide of the surveillance behemoth. And they are *individual* acts, performed for the most part in secrecy. But other, more overt strategies are possible.

The south coast town of Brighton is not normally associated with direct action in any shape or form. But on 10 May 1997, two hundred individuals joined together in what was Britain's first coordinated attack on a CCTV camera system. According to one activist magazine, 'Public ridicule of surveillance cameras is effective in diminishing their power – and more importantly their dignity – and making them highly visible to people who have simply got used [to them] as street furniture.'[11] The protestors were creative in their approach: over 2,000 black and yellow posters carrying the words 'WARNING You Are Being Watched By Closed Circuit Television' were stuck up in toilets and other public spaces, provoking argument and indignation; lasers were used to 'blind' the cameras; posts carrying the cameras were 'occupied'; one camera was hoodwinked with a bag; the highlight of the day came 'when a blow-up doll, the sort available from sex shops, was hoisted to the top of a camera pole and

some rather embarrassed firefighters were dispatched with their ladders to remove her'.[12]

The protestors demonstrated a sophisticated knowledge of both the psychology and the technology of CCTV:

> More fun can be had trying to destabilise the confidence in the relationship between the camera operator and the police on the ground. For example, some sea-front boy racers were caught pouring liquid from a petrol can onto a car in front of a CCTV camera. When the police raced to the scene, the lads got out some sponges and said they were just cleaning it (the can contained water) ... Making plays in front of a range of cameras simultaneously sends a direct message to the control room that we are watching them watching us. Identical masks can be used for protection and confusion ... Many cameras use microwaves to send information back to the central control room, and these can be disabled using reflective industrial foil strips attached to helium-filled balloons at the correct height. Camera poles can be useful 'Lost Children Stations'. Simply make a sign and give balloons to children waiting under the cameras. Now who would take a balloon off a child?

But despite the satisfaction such demonstrations engender, we should not fool ourselves. Present resistance efforts are better than nothing, but they still take place within a general and growing surveillance environment – small victories do not equate to a dismantling of the panoptic whole. 'Who will watch the watchers?' is a critical question; but then, so is 'Who will watch the watchers of the watchers?' and so on *ad nauseam*. The truth is that even with the biggest budgets, the most advanced technology and the best will in the world, no system we can set in place will be invulnerable to subversion. Human ingenuity combined with human craving for superiority and power will

always find a way around restrictions. Examples abound: the Constitution of the United States of America explicitly states that control of the nation's money supply should rest with the state. And yet we have a private bank (the cunningly named Federal Reserve, which has nothing to do with the US government and can be found, should you choose to look, among the white 'business pages' of the US telephone directory), co-owned by seven private banks, at least three of whom are not even US entities, doing just that and essentially dictating the economy of the USA. Despite appearances to the contrary, Alan Greenspan and his successors are private businessmen to a man.

That such a subterfuge can be perpetrated on the American people, against the explicit prohibition of the Constitution, is a timely 'heads-up' to all those concerned with the intrusive nature of modern corporate and governmental structures; we must beware of taking appearance for substance, of confusing high-sounding declarations, voluntary codes and toothless legislation for effective regulation and relevant laws that will vigorously pursue any miscreant with custodial deterrent sentences. The surveillance network is huge, and continues to expand and pry into ever more sensitive areas of our lives. Only comprehensive legislation, and the outright banning of some of its more intrusive offshoots, will control surveillance's worst excesses. Individuals and pressure groups can help cut holes in the surveillance web, but until public opinion sets its weight behind such lone voices, it will be difficult indeed to stem the tide. As Ericson and Haggerty have pointed out: 'In the face of multiple connections across myriad technologies and practices, struggles against particular manifestations of surveillance, as important as they might be, are akin to efforts to keep the ocean's tide back with a broom – a frantic focus on a particular unpalatable technology or practice while the general tide of surveillance washes over us all.'[13]

"Sousveillance"

Inverse Surveillance in Multimedia Imaging

Steve Mann
Dept. of Electrical and Computer Engineering
University of Toronto
Toronto, Canada
mann@eecg.utoronto.ca

ABSTRACT

This is a personal narrative that began 30 years ago as a childhood hobby, of wearing and implanting various sensors, effectors, and multimedia computation in order to re-define personal space and modify sensory perception computationally. This work involved the creation of various computational seeing aids that evolved into a new kind of visual art, using multimedia cyborglogs. Becoming at one with the machine, the author was able to explore a new humanity at the nexus of cyberspace and the real world. The author presents what was discovered accidentally, as a result of facing "cyborg discrimination". In particular, over the past 30 years, peer discrimination has decreased, while institutional and organized discrimination has intensified. Most notably, it was discovered that cyborg discrimination was most intense in establishments having the most surveillance. Rather than avoid such establishments, the author was able to explore and capture unique aspects to understand surveillance in new ways. The word *sur-veillance* denotes a God's eye view from on high (i.e. French for "to watch from above"). An inverse, called sous-veillance (French for "to watch from below") explores what happens when cameras move from lamp posts and ceilings down to eye level. Finally, it is suggested that new personal multimedia technologies, like mass-produced wearable cameraphones, can be used as tools for artists to explore "equiveillance" by shifting this equilibrium between surveillance and sousveillance with inverse/reverse accountability/recountability/continuability of continuous sur/sousveillance.

Categories and Subject Descriptors

J.5 [**Computer Applications**]: ARTS AND HUMANITIES—*Fine arts*

General Terms

Design, Experimentation, Performance, Theory, Verification

Keywords

surveillance, inverse surveillance, sousveillance, weblog, cyborglog, computer mediated reality, eyetap, equiveillance, terrorism, guerrorism, survey, sousvey, perveillance

MM'04, October 10-16, 2004, New York, New York, USA.

What is sousveillance?

SURveillance ("eye-in-the-sky") versus SOUSveillance: bringing cameras from the heavens, "down to earth".

The word "Surveillance" is French for "to watch from above". It typically describes situations where person(s) of higher authority (e.g. security guards, department store owners, or the like) watch over citizens, suspects, or shoppers. The higher authority has often been said to be "Godlike" rather than down at the same level as the individual party or parties under surveillance [Foucault 1977]. In this paper, surveillance is defined as the capture of multimedia content (audio, video, or the like), by a higher entity that is not a peer of, or a party to, the activity being recorded.

The author has suggested "sous-veillance" as French for "to watch from below". The term "sousveillance" refers both to hierarchical sousveillance, e.g. citizens photographing police, shoppers photographing shopkeepers, and taxicab passengers photographing cab drivers, as well as personal sousveillance (bringing cameras from the lamp posts and ceilings, down to eye-level, for human-centered recording of personal experience).

It should be noted that the two aspects of sousveillance (hierarchy reversal and human-centeredness) often interchange, e.g. the driver of a cab one day, may be a passenger in someone else's cab the next day.

Thus a main feature of "sousveillance" as a tool for multimedia artists is effortless capture, processing, storage, recall,

and transmission of an activity by a participant in the activity.

Disclaimer the role of the individual artist and personal passion outside the traditional academic laboratory: Because this paper describes the author's own personal experiences of inventing, designing, building, and living with a variety of body borne computer-based visual information capture, processing, and mediation devices in everyday life, there is a necessary narrative element that would be diminished if it were forced to conform to the objectivity usually found in a scholarly article.

The practice beginning in the author's childhood, involved 30 years of bearable (wearable, implantable/dermaplantable, and body/brain modification) systems and devices. This practice would outstrip a normal ethics review process, so a certain element of this work reaches beyond the traditional manner of scientific explorations, perhaps more into the domain traditionally reserved for the Fine Arts. The arts is one of the few places where there exists an accepted practice of performance art, body art, body modification (like the sex change experiment of Professor Sandy Stone, Eduardo Kac's microchip implanted in the body[1], the "Cyborgian Primitives" movement), and the like.

0.1 Computer Mediated Reality

Since the 1970s the author has been exploring electronically mediated environments using body–borne computers. These explorations in Computer Mediated Reality were an attempt at creating a new way of experiencing the perceptual world, using a variety of different kinds of sensors, transducers, and other body–borne devices controlled by a wearable computer [7].

0.2 Practical Applications

Early on, the author recognized the utility of computer mediated perception (computationally modified presentation of sensory data). For this kind of work, the author invented a device that intercepted rays of eyeward bound light, and resynthesized (typically with a computer-controlled laser) substitute rays so that the resynthesized rays could be collinear with the measured rays. This resulted in a device where three elements existed at the same point in space: (1) the effective center of projection of a camera or other sensor; (2) the convergence point of the above collinear rays of light; and (3) at least one eye of the wearer. Thus the device is equivalent to putting both a camera and a display inside the eye. Such a device, fitted to one or both eyes, is called an EyeTap device [7].

EyeTap devices can be used for electric seeing aids, or when used together with a similar device called the EarTap, for converting the body, in effect, into a camera phone.

0.3 Personal Safety Device

The author's mediated reality devices also included the capability of lifelong capture and transmission of physiological signals together with the EyeTap signal. Capture of the data can allow such a system to function much like the "black box" flight recorder in an aircraft that provides evidence as to why an accident or deliberate violent act occurred.

To protect the data of the "black box" life recorder from accidental or malicious damage, the data has generally been transmitted and recorded at remote locations. Additionally, for example, transmission of synchronized timestamped ECG data allows a remote physician to observe not only the electrical heart activity, but also the visual environment which may provide clues as to environmental causes of ECG irregularities such as arrhythmia.

When it is worn continuously (e.g. out of medical necessity to capture valid data) the long-term adaptation to seeing through the device also provides a unique opportunity to capture, process, store, and recall visual memories. Unlike a mere wearable camera, the EyeTap, because it becomes a manner of seeing, captures exactly what the bearer does see. This results in a new kind of EyeTap cinematographic vision, together with a serendipitously generated logfile that happens without conscious thought or effort.

A cyborg (in the Manfred Clynes sense of a technological synergy that doesn't require conscious thought or effort), can thus generate a lifelong logfile for personal experience capture. Such a logfile is called a cyborglog (http://en.wikipedia.org/wiki/CyborgLog).

Later with the advent of the World Wide Web cyborglogs also became weblogs [Ito 2004], an example of which is shown in Fig 1.

Ironically, the coverage of the East Campus fire (Fig 1) resulted in negative press
Wearable Web Camera Goes Too Far, Anders Hove, Executive Editor,
www-tech.mit.edu/Issue/V116/N28/mann.28c.html from the very paper that might have used the pictures captured in the cyborglog. It is interesting to note that Hove's first main objection was the strange physical appearance (to use his words it's "worse than Spandex, tweed, and bell-bottoms combined"), rather than the privacy issues. This was an objection also raised when the author had driver's license pictures and passport pictures taken, and finally succeeded in making a legal argument as to why self-modification of physical appearance must be accepted, after which a number of passports and driver's licenses were issued with the author's newly created physical appearance.

In particular, living within a permanently installed/instilled photographic perspective allows the bearer to capture precious yet serendipitous moments in life, such as the birth of a newborn, or baby's first steps.

0.4 Related work

Despite the initial negative reactions, a lot of good came of the explorations in web-based cyborglogs (time-stamped diaries of serendipitous personal experience recordings made available to the world). Others are also now proposing similar projects. Industry is also recognizing the importance of inverse surveillance. For example, the Hitachi Design Center in Milano recently sponsored an event entitled "*Applied Dreams Workshop 3: 'Surveillance and Sousveillance*".

Nokia is planning a "life 'blog" (lifelong weblog) product similar to the author's life 'glog (lifelong cyborglog) project. Microsoft's "sensecam" and "MyLifeBits" projects (http://research.microsoft.com/CARPE2004/) and Hewlett

[1]Others, such as Kevin Warwick, have also followed in Kac's footsteps, some for artistic reasons like Kac, and others for more utilitarian reasons.

Figure 1: In this cyborglog, the author encountered an event serendipitously through ordinary everyday activity. As it turned out later, the newspapers had very desperately wanted to get this event covered, but could not reach any of their photojournalists in time to cover the event. The author, however, was able to offer hundreds of pictures of the event, wirelessly transmitted, while the event was still happening. Furthermore, a collaboration with a large number of remote viewers enabled a new form of Computer Supported Cooperative Journalism.

Packard's "Casual Capture" project also build upon various concepts of sousveillance.

Sousveillance is related (even if by inverses) to the tradition of surveillance, and to the artistic practice explored by artists, such as Julie Scher, and the Surveillance Camera Players, among others, working in the medium of surveillance.

Organizations such as Future Physical are also "stretching technology a human adventure" and developing "cultural program exploring boundaries between virtual and physical", e.g. "How will the human body interact with digital tools in the future?". See for example, Wearable Computing Links,
www.futurephysical.org/pages/content/wearable/links.html

In relation to the Fine Arts, the continuous nature of sousveillance (i.e. continuous archival of personal experience) is very much like the concept of "living art". Tehching defined "living art" performances as being of one year in duration (e.g. Tehching Hsieh and Linda Montano held opposite ends of a rope but never touched each other for one year), although other durations are possible (e.g. Montano's 14 year long clothing colour experiments, wearing only one colour of clothing for each of the 14 years, etc.). The author's 30 year long exploration and 20 year long actual experiment in bridging the gap between cyberspace and the real world by living day-to-day life through the electric eyeglass is thus an example that might also be considered part of the tradition of "living art".

Moreover, recently there has been a growing sousveillance industry, with three workshops, organized independently, but around the same time:

- International Workshop on Inverse Surveillance (IWIS 2004), April 12th. This workshop is based on 3 years of planning and previous "inverse conferences" entitled DECONference 2001, DECONference 2002, and DECONference 2003. See, for example,
http://wearcam.org/iwis/ and http://deconference.com
- Memory and Sharing of Experiences, in cooperation with Pervasive 2004, April 20th, 2004, Vienna, Austria. See, for example,
www.ii.ist.i.kyoto-u.ac.jp/ sumi/pervasive04/
Sumi, for example, makes the distinction between surveillance (sensors in the environment) and sousveillance (sensors attached to persons) through the use of "the term 'ubiquitous' to describe sensors set up around the room and 'wearable' to specify sensors carried by users"[9]. Some of this work also relates directly to computer mediated reality [4][2].
- Continuous Archival and Retrieval of Personal Experiences (CARPE 2004), New York, New York, October 15th 2004, held in conjunction with the conference in which this paper appears (ACM Multimedia).

The work presented in this paper is distinct from that of the sousveillance industry which is not focused on art, or the related philosophical and technosocial issues. Likewise, much of the existing work in performance art, and body art is not directly connected to the sousveillance industry, in terms of tools for art and **in**ter**vention**. Thus there is a largely unfulfilled need for such tools.

While it is well known that technology influences art, (e.g. Scher's surveillance-based art is obviously influenced by surveillance technologies), it is hoped that art will also influence technology [1], and in particular, it is hoped that art will influence the growing sousveillance industry as much as the surveillance industry has influenced art.

1. COMPUTER MEDIATED REALITY AS A TOOL FOR TRANSFORMING EVERYDAY LIFE INTO VISUAL ART

Stepping beyond the obvious practical uses of Computer Mediated Reality, there is a more existential motivation regarding how we, as humans, are able to choose the manner in which we define ourselves [10]. The lifelong cyborglog recorder is more than just a visual memory prosthetic. It is also a new tool for the visual arts.

One of the author's original goals of Computer Mediated Reality was to create a body–borne wireless sensory environment which, although technically sophisticated, would function more in the spirit of an artist's personal notes or a painter's canvas. Thus computer-mediated reality was a form of artistic exploration.

In the early 1980s the author was asked to exhibit his computer mediated visual experiences in various art galleries, resulting in a genre of photographic memory characterized by the computer mediation, capture, sharing, recording, and processing of everyday visual experiences. See Fig 2.

These images were created using a concept of vector spaces made from photographic quantities, that the author called "painting with lightvectors".

(a) (b) (c)

Figure 2: Living in a computer mediated environment as a new way of seeing the world as visual art (a) A mid 1980s view of a corridor at McMaster University, and (b) of the Mann residence. (c) Computer mediated view of a television placed on an easel at the base of a commonly photographed space, Niagara Falls. Reality once mediated through television, is again mediated through the wearable computer, as a form of social commentary on what is reality.

Briefly summarized, lightvector paintings are made by combining differently illuminated exposures of the same subject matter, as illustrated in Fig. 3.

This process of "painting with lightvectors" was also possible with a group of people wearing computerized seeing aids that were tuned to the same virtual channel, so that there was a shared computer-mediated visual reality. In this way, the team experienced a collectively modified view of the world, in the production of visual art. Such early apparatus was more cumbersome, however, and thus perhaps less well suited to widespread use as a tool for multimedia artists. (See Fig 4(a).)

More recently, versions of this system have been made available for others to use, with computer programs that can be downloaded from comparametric.sourceforge.net and run on less cumbersome systems, easily made from mobile (small 12 volt automotive) computers, as shown in Fig 4(b). This new tool for artistic exploration is very easy to use, and can be taught in just a few minutes, to anyone with no prior experience. The new hand-held form factor can also be passed around quickly among a group of individuals, so that they can all feel like they are participating in the use of the tool. The grip, similar to the rubber grip of a hammer, makes the tool easy to pass from one person to another, and thus it is very suitable for teaching large groups of students.

2. CYBORG DISCRIMINATION: ACCIDENTAL DISCOVERIES IN SOUSVEILLANCE

By the summer of 1985 the author had built a wearable computer mediated reality system into a jacket, which he wore in much of his day-to-day life.

This resulted in two kinds of public reactions:

- peer discrimination from individuals, either to the outward appearance while wearing the entire system, or the discrimination that remained when the outwardly visible portions were removed, leaving only the permanently attached electrodes, subdermal and dermaplant[2] portions of the apparatus (e.g. with regards to the portions of the apparatus that are permanently attached to the body being seen by others during communal change of clothes for high school gym class, the need to wear a full-body bathing suit to cover dermaplants during swims, or the like);
- official discrimination by representatives of large organizations, allegedly acting on the wishes of the organization. This discrimination pertained to both the unusual outward appearance of the apparatus, the functionality of the apparatus (evidence capture, live transmission of visual images of the official and the officials establishment, etc.), as well as the inward appearance of the body even when the main portion is removed (permanently attached electrodes, subdermal and dermaplant portions of the apparatus that might become visible in an airport stripsearch room).

The author discovered these various elements of discrimination by accident, simply through the process of living the bearable (wearable/implantable) computing lifestyle. Of the various forms of discrimination, the author could forsee the day when the apparatus would no longer have an unusual appearance, because miniaturization would some day allow all of the apparatus to be implanted (and concealed) within the body. Ten to twenty years later, this vision was to have been realized simply by the miniaturization of the apparatus into what appear like ordinary clothing and eyewear (Fig 5).

To achieve such a concealment opportunity, the author invented a new kind of eyeglass design in which the frames come right through the center of the visual field. With materials and assistance provided by Rapp optical, eyeglass frames were assembled using standard photochromic prescription lenses drilled in two places on the left eye, and

[2]Dermaplants refer to devices such as subdermal electrodes, transdermal wound closure, connections on deliberately self-inflicted wounds for purpose of making better connections, and other devices permanently attached to, on, or below the surface of the skin. The author finds that Dermabond (TM) wound closure material manufactured by Closure Medical is often useful for making, growing, or maintaining dermaplants.

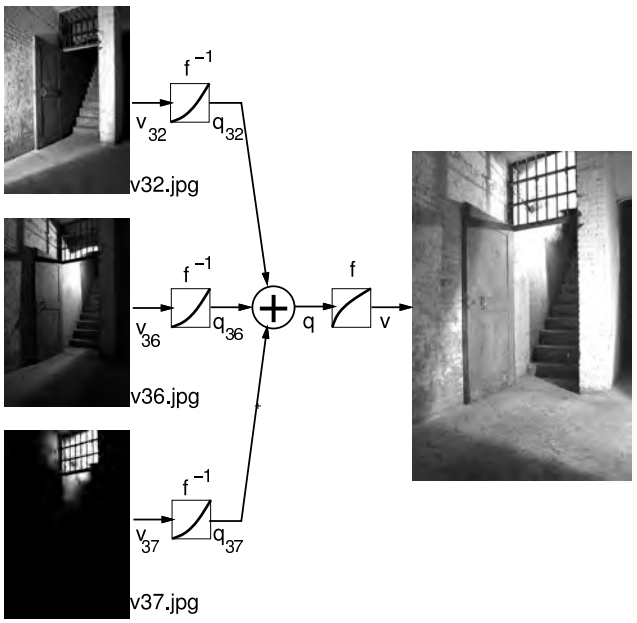


Figure 3: Painting with lightvectors: A lightvector painting is made from various exposures to different sources of illumination. In, for example, v32.jpg, the open basement door under cell block "A" on Alcatraz Island, is exposed to light from a flash lamp held to the left. The flash lamp is then moved to the right, to illuminate the scene from the right, in exposure v36.jpg. Finally, exposure v37.jpg captures light coming from upstairs, beyond the jail bars above the door. Each such picture is displayed on the eyepiece of the author's wearable computer, as the author walks around in the space, illuminating the space from various viewpoints. These pictures are then converted into lightspace by applying an estimate of the inverse of the camera's photographic response function[6]. The resulting photographic quantities are added together, and the combined exposure is then converted from light space back into a picture. (C) Copyleft, S. Mann, 1993.

four places on the right eye, to accommodate a break in the eyeglass frame along the right eye (the right lens being held on with two miniature bolts on either side of the break). The author then bonded fiber optic bundles concealed by the frames, to locate the camera and aremac in back of the device.

The eyeglasses of Fig 5 were crude and simple. A more sophisticated design uses a plastic coating to completely conceal all the elements, so that even when examined closely, evidence of the EyeTap is not visible.

The peer discrimination by the masses was also simply seen as a matter of education and acceptance. The author found that this form of discrimination began to decline sharply in the mid 1980s (beginning around 1984, amid the new-wave androgyny where transhumanism began to take acceptance first in the transgender community and then in society as a whole).

By the 1990s, such peer discrimination had largely disappeared, yet the organizational discrimination continued to increase and intensify. For example, recently, the author was physically assaulted by a number of security guards at the Art Gallery of Ontario. Rather than asking the author to leave, the guards simply pushed the author out of the gallery. The author later asked the Chief Curator as to the

(a) (b)

Figure 4: **(a) Early tools for lightvector paintings:** Jacket based computer system that was completed in the summer of 1985 was used in conjunction with a 2.4 kJ flashlamp in a 14 inch (356mm) reflector. Three separate long communications antennas are visible, two from the backpack and one from the jacket based computer. **(b) A user-friendly mass-produced tool for artists to use provides clear step-by-step instructions on a TV screen that's attached to a light source**. The TV (a standard NTSC TV) attaches to the bottom of the handgrip, and a standard electronic flash attaches to the top. A mobile (12 volt automotive) computer at the base station and the TV on the hand grip eliminate the need for a cumbersome wearable computer system typical of the 1970s and early 1980s lightvector painting systems. Computer programs to make it work are freely available at comparametric.sourceforge.net

reason for this action. The reason given was a possibility of copyright infringement.

This raises an important question as to the right to fair use of one's personal environs, and personal experiences, especially in view of an acquired dependence on computerized visual memory. It seemed the author had unwittingly come to confront, explore, and understand issues concerning the ownership of space and whether such ownership should provide an advantage in perpetrating copyright infringement (i.e. what if their surveillance cameras capture a picture of art that a patron is wearing, such as a painting on a T-shirt — does that justify the patron smashing up their surveillance cameras because of the mere possibility of copyright infringement?). It also raises questions pertaining to the relative worth of humans and walls (e.g. a painting hung on a wall gets more protection tha a painting worn on a T-shirt).

Physical assault in response to a mere potential for copyright infringement seems specious at best, given recent Supreme Court rulings allowing photocopiers in libraries, despite the fact that they *could* be used beyond the level permitted by *fair use*.

This response from the gallery, and other similar institutions has actually *increased* not decreased the amount of recording done:

- Before such incidents the author used to make seeing aids that did not necessarily record;
- now any seeing aid that we make in our lab is equipped with a retroactive record capability. This helps the wearer keep an evidence log in case such violence occurs.

The irony, therefore, in such physical assaults is that the fears of the security guards are coming to fruition by way of their own actions. Similarly, one would expect that if people went around smashing up surveillance cameras with baseball bats, this would probably cause more to be installed,

Figure 5: Fully functional electronic eyeglasses built into wire frames. Eyeward–bound light is diverted along the right temple by way of a fiber bundle, into a miniature camera. A laser directs light along another fiber system on the left temple to redraw the modified reality onto the retina. The details are provided in [7].

and would cause more detailed recordings of each one to be made. It is therefore futile to resort to violence as a means of suppressing evidence gathering technologies.

Thus the fundamentally most difficult element of discrimination appeared to be the official discrimination based on functionality of the cyborg.

The author began to understand this discrimination throughout the 1970s and early 1980s, as being correlated to the degree of surveillance present in an establishment. It appeared, for example, that the establishments where official discrimination was greatest, were the very same establishments where the use of video surveillance was the greatest.

Therefore the author, through simply a personal desire to live in a computer mediated world, encountered hostilities from paranoid security guards, seemingly afraid of being held accountable. It seemed that the very people who pointed cameras at citizens were the ones who were most afraid of new inventions and technologies of citizen cameras.

The harsh and sometimes hostile discrimination against the author, by officials, security guards, and representatives of large organizations led the author to begin thinking mainly about official discrimination against cyborg functionality. In order to learn from these hostilities, the author wished to understand this discrimination by applying the scientific method, within an ethnomethodological sense, which evolved into using body-borne multimedia computation as a tool for social inquiry and *action research* [3][8] on surveillance as an emergent agenda. However the unique framework and situation did not conform to a particular academic discipline (psychology, sociology, science, engineering, etc.). Therefore this work was often appreciated more within the arts community, where interdisciplinarity was fully embraced even many years ago.

Various places that the author was most strongly prohibited from entering seemed to include places like maffia run gambling casinos, pawnshops where money laundering might be taking place, and jewellery stores. Such organizations were ironically the places where surveillance cameras were abundant.

Along another avenue of discourse, the author began to undertake a series of explorations in which he unwittingly became what others referred to as an "artist", despite having a more science and engineering based background.

This exploration into the Fine Arts arose from a desire to try to understand the reasoning behind such organizational discrimination, rather than simply avoiding it.

For example, as a departure from EyeTap eyeglasses as seeing aids, the author also constructed various forms of cyborg jewellery, in order to test an hypothesis, namely that jewellery store owners would welcome and appreciate having pictures taken by innovative jewellery. Thus the author built Personal Safety Devices (PSDs) into jewellery (Fig. at top of first page of paper). The reaction was quite surprising. Even when blatantly told that the devices contained a camera, jewellery store and pawnshop owners did not object to the device in any way. Although the device does not allow the wearer to live in a computer mediated world, it captures all the elements of paranoia that the officials most feared, e.g. primarily a video captured record of their establishment and activities. Yet they accepted this alternative form of the device without complaint, largely because it so nicely landed within **their** genre. Indeed, many of the jewellery store owners wanted to commercialize and sell the sousveillance necklace and other domewear products.

The sousveillance necklace established a more inclusive narrative that treated the store clerks and security guards as colleagues. As a sharp departure from 20th century "us versus them" thinking, the cyborglog jewellery created a new kind of artistic practice and discourse. By presenting it as an object that the guards and shopkeepers could try on, and look at themselves in the mirror wearing, they had no problem with it being in their store, transmitting images to the World Wide Web. It is therefore interesting to note that an inclusionary rather than exclusionary element of sousveillance is possible. While surveillance tends to be exclusionary, and tends to present a very strong "us versus them" directionality, sousveillance can be made to operate much more like Peer-to-Peer, in the sense of creating a level playing field. The sousveillance landscape therefore may include both shoppers and shopkeepers, wearing personal recording devices. Moreover, a shopkeeper may then assume multiple roles, e.g. one role is obedience to a store manager, but another role might be the capture of his or her own personal "day in my life at work" cyborglog to share with friends.

2.1 Schrodinger's Cam: Nonwillful blindness with the maybecamera

Another aspect of artistic discourse and philosophical exploration was the reflectionism [5] of uncertainty (Fig 6). A large number of wireless webcam shirts were made, but only some of them had cameras in them. They were then shuffled and distributed widely. Honestly not knowing whether or not one was wearing a camera added a new dimension to putting the uncertainty principle into artistic practice. Moreover, consider, for example, the "sousveillance underground" as a probe into New York proposed ban on pho-

(a) (b) (c) (d) (e)

Figure 6: **Heisenberg Uncertainty with Schrodinger's Cam: The Maybecamera.** A large number of wireless webcam shirts were made, but only some having cameras. These were shuffled so each wearer did not know whether or not theirs had a camera in it. (a) Closeup picture of one of many maybecameras showing a detournement, reversalism/reflectionism, and deconstruction of the typical language (text) of surveillance. (b) A number of people wore these gambling (e.g. Casino Niagara, etc.) without incident. This suggests that perhaps the guards don't read shirts. The wearer's don't know which shirts contain wearable wireless web cameras and which shirts don't. (c) The author's maybecamera design is spreading around the world. Dr. S. Pantagis, a physician at a New York hospital, made an initial batch of 25 of these to distribute to New York poets, followed by a larger production run. (d) as seen in a New York department store's security camera. (e) closeup view seen by security camera.

Figure 7: The international Workshop on Inverse Surveillance was an intimate gathering, limited to 30 participants from around the world, and held in three small rooms like that shown above. There were 3 simultaneous tracks: Philosophy of souveillance; sousveillance industry and business opportunites; and existemology (epistemology of self determination).

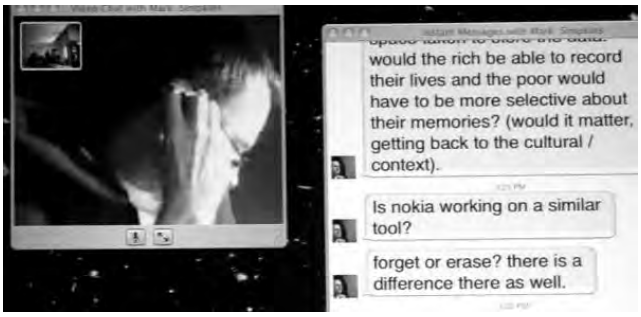


Figure 8: A number of participants were also remotely present from around the world.

tography in subways. An exhibit of subway photographs is expected to follow.

3. (DE)CONCLUSIONS: THE NEED FOR FURTHER INQUIRY

Computer-mediated reality, with its origins as a tool for lightvector painting, has been presented as a new tool for visual artists. In particular, the personal experience capture of sousveillance is useful both to see the world in a different light, as well as to challenge our preconceived notions of an otherwise one-sided surveillance-only society.

However, the concepts of sousveillance raise many questions that cannot be answered in a single paper. It is therefore hoped that it will create a broader intellectual landscape, and a basis upon which to build many different research directions.

Arising out of a 2001 event, the author began a collaboration with Samsung on a conference entitled "Sousveillance Fusion 2002", which eventually led to a series of conferences, in 2002, 2003, and a smaller workshop in 2004 (Fig 7 and 8).

The goal of this workshop was not so much to solve the technical problems (many of which have already been solved many years ago), but to address the problems that an individual, working alone, could never solve. These fundamental problems are the technosocial problems; for this we need large scale collaboration.

One important result of the discussion was a better understanding of the shifting equilibrium between surveillance and sousveillance, as outlined in the **Equiveillance Table** below:

Surveillance	Sousveillance
God's eye view from above. (Authority watching from on-high.)	Human's eye view. ("Down-to-earth.")
Cameras usually mounted on high poles, up on ceiling, etc..	Cameras down-to-earth (at (ground level), e.g. at human eye-level.
"Eye in the Sky" (i.e. camera in the sky)	"Eye in the Eye" (i.e. eye is the camera)
Sur-veiller is French for "to watch from above".	Sous-veiller is French for "to watch from below".
Architecture-centered (e.g. cameras usually mounted on or in structures).	Human-centered (e.g. cameras carried or worn by, or on, people).
Recordings made by authorities, remote security staff, etc..	Recordings of an activity made by a participant in the activity.
Note that in most states it's	In most states it's legal to

illegal to record a phone conversation of which you are not a party. Perhaps the same would apply to an audiovisual recording of somebody else's conversation.	record a phone conversation of which you are a party. Perhaps the same would apply to an audiovisual recording of your own conversations, i.e. conversations in which you are a party.
Recordings are usually kept in secret.	Recordings are often made public e.g., on the World Wide Web.
Process usually shrouded in secrecy.	Process, technology, etc., are usually public, open source, etc..
Panoptic origins, as described by Foucault, originally in the context of a prison in which prisoners were isolated from each other but visible at all times by guards. Surveillance tends to isolate individuals from one another while setting forth a one-way visibility to authority figures.	Community-based origins, e.g. a personal electronic diary, made public on the World Wide Web. Sousveillance tends to bring together individuals, e.g. it tends to make a large city function more like a small town, with the pitfalls of gossip, but also the benefits of a sense of community participation.
Privacy violation may go un-noticed, or un-checked. Tends to not be self-correcting.	Privacy violation is usually immediately evident. Tends to be self-correcting.
It's hard to have a heart-to-heart conversation with a lamp post on top of which is mounted a surveillance camera.	At least there's a chance you can talk to the person behind the sousveillance camera.
When combined with computers, we get ubiquitous computing ("ubiqcomp") or pervasive computing ("pervcomp"). Perveillance (ubiq./perv. comp) tends to rely on cooperation of the infrastructure in the environments around us.	When combined with computers, we get wearable computing. ("wearcomp"). Wearcomp usually doesn't require the cooperation of any infrastructure in the environments around us.
With surveillant-computing, the locus of control tends to be with the authorities.	With sousveillant-computing, it is possible for the locus of control to be more distributed. and, in particular, to rest with the individual.

A larger symposium on sousveillance is planned for 2005.

More is written on sousveillance as the paper corresponding to the keynote address at a workshop attached to this ACM Multimedia conference, entitled "Continuous Archival and Retrieval of Personal Experiences" (CARPE). In that 20 pape paper, related concepts of sur/sousveillance, equiveillance, and auditor/viditor relationships are described, together with EyeTap device invention, design, and realization.

4. ACKNOWLEDGEMENTS

I'd like to thank my many past and present students, in particular, James Fung, Corey Manders, Daniel Chen (dusting), Mark Post (sequencer), Chris Aimone, and Anurag Sehgal (keyer), who've tolerated and contributed to the growth of the artistic practice of sousveillance, as well as Alex Jaimes who has made many useful suggestions on the original and revised manuscripts. I'd also like to acknowledge our many sponsors, including Nikon, for supplying the camera systems, and Daymen Photo, for supplying the Metz Mecablitz units used in our lightvectoring art.

5. GLOSSARY OF NEW TERMS

- Côteveillance (also known as coveillance): People watching people, i.e. the specific aspect of sousveillance that pertains directly to *peer to peer* monitoring and recording of activities by another at the same level of social hierarchy.
- Equiveillance: The equilibrium (balance) between surveillance and sousveillance.
- Existemology (portmanteau of Existential Epistemology): An epistemology of choice and metaphysics of freewill that typically arises from self-constructed reality intermediaries. Examples include the learning process that arises from the computationally modified sensory input of a self-constructed electric seeing aid.
- Guerrorism (Portmanteau of Guerre and Terrorism): The unlawful use of authority, by a security guard, garrison, or watch, for the purpose of intimidating civilians or citizens into support for, or compliance with, a war, such as a "war on terrorism", "war on crime", "war on (the) disease(d)", "war on (some) drugs", or the like.
- Perveillance: Pervasive surveillance, typically attained through the use of pervasive or ubiquitous computing.
- Sousveillance (undersight): (1) The recording of an activity by a participant in the activity, typically by way of a human-borne camera; (2) Inverse surveillance (also known as reverse surveillance or inverted surveillance), i.e. the recording or monitoring of a high ranking official by a person of lower authority.
- Sousvival: A sustained existence through low intensity peacefare. To actively seek ways of continued living without killing others.

6. REFERENCES

[1] The influence of art and design on computer science research and development. In W. J. Mitchell, A. S. Inouye, and M. S. Blumenthal, editors, *The Influence of Art and Design on Computer Science Research and Development*, chapter 4. National Academy of Sciences, 2003. http://bob.nap.edu/html/beyond_productivity/ch4.html.

[2] K. Aizawa, T. Hori, S. Kawasaki, and T. Ishikaw. Capture and efficient retrieval of life log. In *Proceedings of the Pervasive 2004 Workshop on Memory and Sharing of Experiences*, Linz/Vienna, Austria, Tuesday, April 20 2004. IEEE Computer Society.

[3] W. Carr and S. Kemmis. *Becoming Critical: Education, Knowledge and Action Research*. The Falmer Press, London, 1986.

[4] A. Frigo. Storing, indexing and retrieving my autobiography. In *Proceedings of the Pervasive 2004 Workshop on Memory and Sharing of Experiences*, Linz/Vienna, Austria, Tuesday, April 20 2004. IEEE Computer Society.

[5] S. Mann. Reflectionism and diffusionism. *Leonardo, http://wearcam.org/leonardo/index.htm*, 31(2):93–102, 1998.

[6] S. Mann. Comparametric equations with practical applications in quantigraphic image processing. *IEEE Trans. Image Proc.*, 9(8):1389–1406, August 2000. ISSN 1057-7149.

[7] S. Mann. *Intelligent Image Processing*. John Wiley and Sons, November 2 2001. ISBN: 0-471-40637-6.

[8] J. Masters. The history of action research. In I. Hughes, editor, *Action Research Electronic Reader*. http://www.behs.cchs.usyd.edu.au/arow/Reader/rmasters.htm.

[9] Y. Sumi, S. Ito, T. Matsuguchi, S. Fels, and K. Mase. Collaborative capturing and interpretation of interactions. In *Proceedings of the Pervasive 2004 Workshop on Memory and Sharing of Experiences*, Linz/Vienna, Austria, Tuesday, April 20 2004. IEEE Computer Society.

[10] S. M. (with Hal Niedzviecki). *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*. Randomhouse (Doubleday), November 6 2001. ISBN: 0-385-65825-7.

Full Text | Blog, Podcast, or Website

Human This Christmas: Tressie McMillan Cottom

Tressie McMillan Cottom. *New York Times (Online)*, New York: New York Times Company. Dec 20, 2022.

The New York Times

Full Text

Everyone in my professional life — fellow faculty members, other writers — is up in arms about ChatGPT, the new artificial intelligence tool that can write like a human being.

Tech is not supposed to be human. It is only ever supposed to be humanoid. But this chatbot can take multiple ideas and whip up a cogent paragraph. The professional classes are aghast.

Some of us professors are primarily obsessed with assessment and guarding the integrity of, well, everything. We scan essays into proprietary cheating detectors and tut-tut when a program finds a suspiciously high proportion of copied text. For at least 10 years, academics have fought about the proper role of rooting out computer-assisted cheating. Should we build better tests or scare students straight like a 1980s after-school special? We are split.

ChatGPT is so good that we aren't sure if using it even constitutes cheating. The paragraphs it offers are original in that they aren't copied from another text. It can even insert citations, protecting our academic culture of credit. Whether accurate or not, inserting references conforms to the style of academic writing. Nature asks if the technology should worry professors.

I would be worried, except my profession has been declared dead so many times that I've bought it a funeral dress. Humanities are not dead. Writing isn't dead. And higher education will hobble along. You know why? For one, because this technology produces really creepy stuff.

A.I. writes prose the way horror movies play with dolls. Chucky, Megan, the original Frankenstein's monster. The monster dolls appear human and can even tell stories. But they cannot make stories. Isn't that why they are monsters? They can only reflect humanity's vanities back at humans. They don't make new people or chart new horizons or map new experiences. They are carbon copies of an echo of the human experience.

I read some of the impressive essays written with ChatGPT. They don't make much of an argument. But neither do all writers, especially students. That's not a tell. A ChatGPT essay is grammatically correct. Writers and students often aren't. That's the tell.

But even when the essays are a good synthesis of other essays, written by humans, they are not human. Frankly, they creep me out precisely because they are so competent and yet so very empty. ChatGPT impersonates sentiment with sophisticated word choice but still there's no élan. The essay does not invoke curiosity or any other emotion. There is a voice, but it is mechanical. It does not incite, offend or seduce. That's because real voice is more than grammatical patternmaking.

Voice, that elusive fingerprint of all textual communication, is a relationship between the reader, the world and the writer. ChatGPT can program a reader but only mimic a writer. And it certainly cannot channel the world between them.

I was in the grocery store this week. Everything is holiday music. I love the different genres of Christmas music. In my life, it isn't the holiday season until the Temptations' "Silent Night" spills from a public speaker. It isn't good enough for me to cue up my own selection; I want other people playing it. I want to hear it in a store or spilling from a Christmas tree park or a car. That's how I know the season still has meaning as a tradition that calls strangers into communion, if only for the few moments when we hum a few bars of "Silent Night" together in a grocery store aisle.

This store was playing a song by a group called Pentatonix. I looked it up to be sure. The song was musically sound, as far as I could tell. The notes were all in the right places. But it had been filtered in the way that mechanical Muzak covers transform actual songs into mere sounds: technical holiday music. And it didn't call anyone into the season, I can tell you that.

That's the promise of ChatGPT and other artificial approximations of human expression. The history of technology says that these things have a hype cycle: They promise; we fear; they catch hold; they under-deliver. We right-size them. We get back to the business of being human, which is machine-proof.

This is a great time to think about the line between human and machine, lived experience and simulation. There are 1,000 holiday traditions. All of them call us back into the space of being more human than machine. Less scheduled, more present. Less technical, and messier.

Humanities, arts and higher education could use a little reminder that we do human. That's our business, when we do it well. We are as safe from ChatGPT as the Temptations are from Pentatonix.

What I Am Up To

I talked with Trevor Noah for his final week hosting "The Daily Show." You can watch our conversation here. Trevor ended his seven-year tenure with an impassioned plea to broaden and deepen our culture's pool of experts. I am smarter because I look for organic genius. Trevor and I share that value.

I recently talked with NPR's "Pop Culture Happy Hour" about the modern western "Yellowstone." There is a fifth season. You may be bingeing the series this holiday season. I don't recommend doing it all in one sitting. The host Linda Holmes and I talked about watching "Yellowstone" like your parents once watched soap operas: in doses, and with a healthy sense of perspective on its latent politics.

What's on My Mind

The Biden administration brought Brittney Griner home and signed the Respect for Marriage Act into law. There is always something to fight about, but these are indisputably good things. Thanks, President Biden.

If we are going to fight, let's let it mean something. The spectacular explosion of FTX and Elon Musk's heel turn at Twitter say it is high time we debate what I have called "scam culture."

Tressie McMillan Cottom (@tressiemcphd) is an associate professor at the University of North Carolina at Chapel Hill School of Information and Library Science, the author of "Thick: And Other Essays" and a 2020 MacArthur fellow.
Word count: 1012

We come to bury ChatGPT, not to praise it.

Mon 06 February 2023

Large language models (LLMs) like the GPT family learn the statistical structure of language by optimising their ability to predict missing words in sentences (as in 'The cat sat on the [BLANK]'). Despite the impressive technical ju-jitsu of transformer models and the billions of parameters they learn, it's still a computational guessing game. ChatGPT is, in technical terms, a 'bullshit generator'. If a generated sentence makes sense to you, the reader, it means the mathematical model has made sufficiently good guess to pass your sense-making filter. The language model has no idea what it's talking about because it has no idea about anything at all. It's more of a bullshitter than the most egregious egoist you'll ever meet, producing baseless assertions with unfailing confidence because that's what it's designed to do. It's a bonus for the parent corporation when journalists and academics respond by generating acres of breathless coverage, which works as PR even when expressing concerns about the end of human creativity.

Unsuspecting users who've been conditioned on Siri and Alexa assume that the smooth talking ChatGPT is somehow tapping into reliable sources of knowledge, but it can only draw on the (admittedly vast) proportion of the internet it ingested at training time. Try asking Google's BERT model about Covid or ChatGPT about the latest Russian attacks on Ukraine. Ironically, these models are unable to cite their own sources, even in instances where it's obvious they're plagiarising their training data. The nature of ChatGPT as a bullshit generator makes it harmful, and it becomes more harmful the more optimised it becomes. If it produces plausible articles or computer code it means the inevitable hallucinations are becoming harder to spot. If a language model suckers us into trusting it then it has succeeded in becoming the industry's holy grail of 'trustworthy AI'; the problem is, trusting any form of machine learning is what leads to a single mother having their front door kicked open by social security officials because a predictive algorithm has fingered them as a

probable fraudster, alongside many other instances of algorithmic violence.

Of course, the makers of GPT learned by experience that an untended LLM will tend to spew Islamophobia or other hatespeech in addition to talking nonsense. The technical addition in ChatGPT is known as Reinforcement Learning from Human Feedback (RHLF). While the whole point of an LLM is that the training data set is too huge for human labelling, a small subset of curated data is used to build a monitoring system which attempts to constrain output against criteria for relevance and non-toxicity. It can't change the fact that the underlying language patterns were learned from the raw internet, including all the ravings and conspiracy theories. While RLHF makes for a better brand of bullshit, it doesn't take too much ingenuity in user prompting to reveal the bile that can lie beneath. The more plausible ChatGPT becomes, the more it recapitulates the pseudo-authoritative rationalisations of race science. It also shows that despite the boast that LLMs are largely self-training, any real world system will require precaritised 'ghost work' to maintain its plausibility. It turns out that AI is not sci-fi but a techologised intensification of existing relations of labour and power. The $2/hour paid to outsourced workers in Kenya so they could be "tortured" by having to tag obscene material for removal is figurative of the invisible and gendered labour of care that always already holds up our existing systems of business and government.

As with the rest of AI, the dangers of ChatGPT go far deeper than bias and discrimination. Despite evidence that the model's powers of 'reasoning' are shallow heuristics based on the frequency of associations in the training data (meaning, as an illustrative example, that it's good at answering 'What is 24 x 18?' and poor at answering 'What is 23 x 18?') there are many in the AI community who insist on imputing emergent properties of reasoning and insight to ChatGPT. Its parent company, OpenAI, was set up "to ensure that artificial general intelligence benefits all of humanity", where 'artificial general intelligence' (AGI) is the insider term used for human-like intelligence that goes beyond narrow AI like facial recognition or self-driving cars. However, as I spell out in my book, the concept of AGI is inseparable from the kind of hierarchy of intelligence that has underpinned ideas of innate supremacy since the days of empire and colonialism. Hardly surprising, then, that the same Silicon Valley cultures that incubate enthusiasm for ChatGPT as emergent AGI also show allegiance to

associated world views like Long Termism, where the immediate vulnerability of millions of ordinary people counts as nothing in relation to the prospects of a future space-faring super race.

In the mean time, OpenAI is acquiring billions of dollars of investment on the back of the ChatGPT hype. The point here is not only the pocketing of a pyramid-scale payoff but the reasons why institutions and governments are prepared to invest so much in these technologies. For these players, the seductive vision isn't real AI (whatever that is) but technologies that are good enough to replace human workers or, more importantly, to precaritise them and undermine them. ChatGPT isn't really new but simply an iteration of the class war that's been waged since the start of the industrial revolution. That allegedly well-informed commentators can infer that ChatGPT will be used for "cutting staff workloads" rather than for further staff cuts illustrates a general failure to understand AI as a political project. Contemporary AI, as I argue in my book, is an assemblage for automatising administrative violence and amplifying austerity. ChatGPT is a part of a reality distortion field that obscures the underlying extractivism and diverts us into asking the wrong questions and worrying about the wrong things. Instead of expressing wonder, we should be asking whether it's justifiable to burn energy at "eye watering" rates to power the world's largest bullshit machine.

Commentary that claims 'ChatGPT is here to stay and we just need to learn to live with it' are embracing the hopelessness of what I call 'AI Realism'. The compulsion to show 'balance' by always referring to AI's alleged potential for good should be dropped by acknowledging that the social benefits are still speculative while the harms have been empirically demonstrated. Saying, as the OpenAI CEO does, that we are all 'stochastic parrots' like large language models, statistical generators of learned patterns that express nothing deeper, is a form of nihilism. Of course, the elites don't apply that to themselves, just to the rest of us. The structural injustices and supremacist perspectives layered into AI put it firmly on the path of eugenicist solutions to social problems.

Instead of reactionary solutionism, let us ask where the technologies are that people really need. Let us reclaim the idea of socially useful production, of technological developments that start from community needs. The post-Covid 'new normal' has turned out to involve both the normalisation of neural networks and a rise in necropolitics.

Transformer models and diffusion models are not creative but carceral - they and other forms of AI imprison our ability to imagine real alternatives. It's not so long ago that we all woke up to the identity of truly essential workers; the people carrying out the precaritised roles of nursing, teaching, caring, delivering and cleaning, the very professions who are being forced to reinvent the idea of the general strike simply to regain the conditions for survival. Instead of being complicit with expensive toys running in carbon emitting data centres, we can focus instead on centring activities of care. As discussed in more detail in 'Resisting AI', a refusal of algorithmic immiseration goes along with a positive search for alternatives, and I lay out a programme of people's councils and commons-based solidarity to do just that. It's not time to chat with AI, but to resist it.

1
Engineered Inequity
Are Robots Racist?

WELCOME TO THE FIRST INTERNATIONAL BEAUTY CONTEST JUDGED BY ARTIFICIAL INTELLIGENCE.

So goes the cheery announcement for Beauty AI, an initiative developed by the Australian- and Hong Kongbased organization Youth Laboratories in conjunction with a number of companies who worked together to stage the first ever beauty contest judged by robots (Figure 1.1).[1] The venture involved a few seemingly straightforward steps:

1. Contestants download the Beauty AI app.
2. Contestants make a selfie.
3. Robot jury examines all the photos.
4. Robot jury chooses a king and a queen.
5. News spreads around the world.

As for the rules, participants were not allowed to wear makeup or glasses or to don a beard. Robot judges were programmed to assess contestants on the basis of wrinkles, face symmetry, skin color, gender, age group, ethnicity, and “many other parameters.” Over 6,000 submissions from approximately 100 countries poured in. *What could possibly go wrong?*

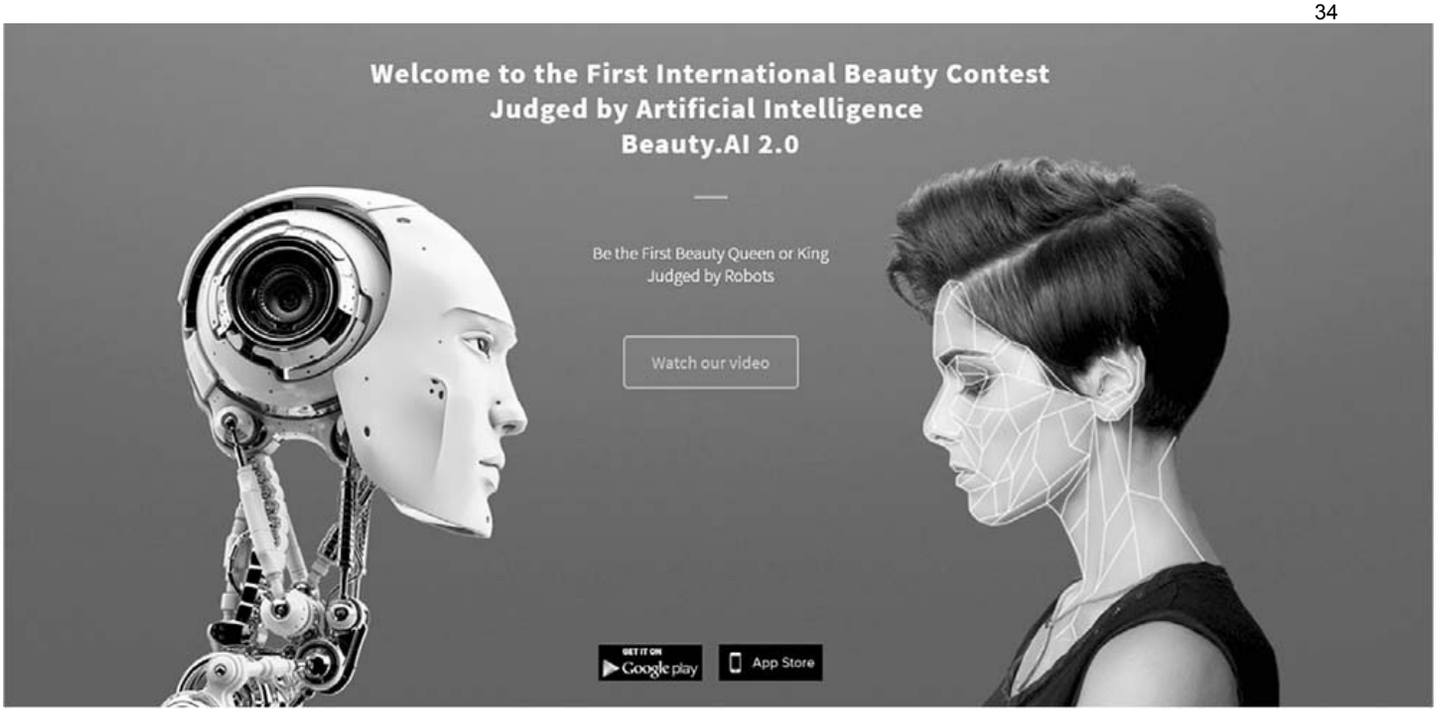


Figure 1.1 Beauty AI

Source: http://beauty.ai

On August 2, 2016, the creators of Beauty AI expressed dismay at the fact that "the robots did not like people with dark skin." All 44 winners across the various age groups except six were White, and "only one finalist had visibly dark skin."[2] The contest used what was considered at the time the most advanced machine-learning technology available. Called "deep learning," the software is trained to code beauty using pre-labeled images, then the images of contestants are judged against the algorithm's embedded preferences.[3] Beauty, in short, is in the trained eye of the algorithm.

As one report about the contest put it, "[t]he simplest explanation for biased algorithms is that the humans who create them have their own deeply entrenched biases. That means that despite perceptions that algorithms are somehow neutral and uniquely objective, they can often reproduce and amplify existing prejudices."[4] Columbia University professor Bernard Harcourt remarked: "The idea that you could come up with a culturally neutral, racially neutral conception of beauty is simply mind-boggling." Beauty AI is a reminder, Harcourt notes, that humans are really doing the thinking, even when "we think it's neutral and scientific."[5] And it is not just the human programmers' preference for Whiteness that is encoded, but the combined preferences of *all* the humans whose data are studied by machines as they learn to judge beauty and, as it turns out, *health*.

In addition to the skewed racial results, the framing of Beauty AI as a kind of preventative public health initiative raises the stakes considerably. The team of biogerontologists and data scientists working with Beauty AI explained that valuable information about people's health can be gleaned by "just processing their photos" and that, ultimately, the hope is to "find effective ways to slow down ageing and help people look healthy and beautiful."[6] Given the

overwhelming Whiteness of the winners and the conflation of socially biased notions of beauty and health, darker people are implicitly coded as unhealthy and unfit – assumptions that are at the heart of scientific racism and eugenic ideology and policies.

Deep learning is a subfield of machine learning in which "depth" refers to the layers of abstraction that a computer program makes, learning more "complicated concepts by building them out of simpler ones."[7] With Beauty AI, deep learning was applied to image recognition; but it is also a method used for speech recognition, natural language processing, video game and board game programs, and even medical diagnosis. Social media filtering is the most common example of deep learning at work, as when Facebook auto-tags your photos with friends' names or apps that decide which news and advertisements to show you to increase the chances that you'll click. Within machine learning there is a distinction between "supervised" and "unsupervised" learning. Beauty AI was supervised, because the images used as training data were pre-labeled, whereas unsupervised deep learning uses data with very few labels. Mark Zuckerberg refers to deep learning as "the theory of the mind … How do we model – in machines – what human users are interested in and are going to do?"[8] But the question for us is, is there only *one* theory of the mind, and *whose mind* is it modeled on?

It may be tempting to write off Beauty AI as an inane experiment or harmless vanity project, an unfortunate glitch in the otherwise neutral development of technology for the common good. But, as explored in the pages ahead, such a conclusion is naïve at best. Robots exemplify how race is a form of technology itself, as the algorithmic judgments of Beauty AI extend well beyond adjudicating attractiveness and into questions of health, intelligence, criminality, employment, and many other fields, in which innovative techniques give rise to newfangled forms of racial discrimination. Almost every day a new headline sounds the alarm, alerting us to the New Jim Code:

"Some algorithms are racist"

"We have a problem: Racist and sexist robots"

"Robots aren't sexist and racist, you are"

"Robotic racists: AI technologies could inherit their creators' biases"

Racist robots, as I invoke them here, represent a much broader process: social bias embedded in technical artifacts, the allure of objectivity without public accountability. Race as a form of technology – the sorting, establishment and enforcement of racial hierarchies with real consequences – is embodied in robots, which are often presented as simultaneously akin to humans but different and at times superior in terms of efficiency and regulation of bias. Yet the way robots can be racist often remains a mystery or is purposefully hidden from public view.

Consider that machine-learning systems, in particular, allow officials to outsource decisions that are (or should be) the purview of democratic oversight. Even when public agencies are employing such systems, private companies are the ones developing them, thereby acting like

political entities but with none of the checks and balances. They are, in the words of one observer, "governing without a mandate," which means that people whose lives are being shaped in ever more consequential ways by automated decisions have very little say in how they are governed.[9]

For example, in *Automated Inequality* Virginia Eubanks (2018) documents the steady incorporation of predictive analytics by US social welfare agencies. Among other promises, automated decisions aim to mitigate fraud by depersonalizing the process and by determining who is eligible for benefits.[10] But, as she documents, these technical fixes, often promoted as benefiting society, end up hurting the most vulnerable, sometimes with deadly results. Her point is not that human caseworkers are less biased than machines – there are, after all, numerous studies showing how caseworkers actively discriminate against racialized groups while aiding White applicants deemed more deserving.[11] Rather, as Eubanks emphasizes, automated welfare decisions are not magically fairer than their human counterparts. Discrimination is displaced and accountability is outsourced in this postdemocratic approach to governing social life.[12]

So, how do we rethink our relationship to technology? The answer partly lies in how we think about race itself and specifically the issues of intentionality and visibility.

I Tinker, Therefore I Am

Humans are toolmakers. And robots, we might say, are humanity's finest handiwork. In popular culture, robots are typically portrayed as humanoids, more efficient and less sentimental than *Homo sapiens*. At times, robots are depicted as having human-like struggles, wrestling with emotions and an awakening consciousness that blurs the line between maker and made. Studies about how humans perceive robots indicate that, when that line becomes too blurred, it tends to freak people out. The technical term for it is the "uncanny valley" – which indicates the dip in empathy and increase in revulsion that people experience when a robot appears to be too much like us.[13]

Robots are a diverse lot, with as many types as there are tasks to complete and desires to be met: domestic robots; military and police robots; sex robots; therapeutic robots – and more. A robot is any machine that can perform a task, simple or complex, directed by humans or programmed to operate automatically. The most advanced are smart machines designed to learn from and adapt to their environments, created to become independent of their makers. We might like to think that robotic concerns are a modern phenomenon,[14] but our fascination with automata goes back to the Middle Ages, if not before.[15]

In *An Anthropology of Robots and AI*, Kathleen Richardson observes that the robot has "historically been a way to talk about dehumanization" and, I would add, *not* talk about racialization.[16] The etymology of the word robot is Czech; it comes from a word for "compulsory service," itself drawn from the Slav *robota* ("servitude, hardship").[17] So yes, people have used robots to express anxieties over annihilation, including over the massive

threat of war machines. But robots also convey an ongoing agitation about human domination over other humans![18]

The first cultural representation that employed the word robot was a 1920 play by a Czech writer whose machine was a factory worker of limited consciousness.[19] Social domination characterized the cultural laboratory in which robots were originally imagined. And, technically, *people* were the first robots. Consider media studies scholar Anna Everett's earliest experiences using a computer:

> In powering up my PC, I am confronted with the DOS-based text that gave me pause … "Pri. Master Disk, Pri. Slave Disk, Sec. Master, Sec. Slave." Programmed here is a virtual hierarchy organizing my computer's software operations … I often wondered why the programmers chose such signifiers that hark back to our nation's ignominious past … And even though I resisted the presumption of a racial affront or intentionality in such a peculiar deployment of the slave and master coupling, its choice as a signifier of the computer's operations nonetheless struck me.[20]

Similarly, a 1957 article in *Mechanix Illustrated*, a popular "how-to-do" magazine that ran from 1928 to 2001, predicted that, by 1965:

> Slavery will be back! We'll all have personal slaves again … [who will] dress you, comb your hair and serve meals in a jiffy. Don't be alarmed. We mean robot "slaves."[21]

It goes without saying that readers, so casually hailed as "we," are not the descendants of those whom Lincoln freed. This fact alone offers a glimpse into the implicit Whiteness of early tech culture. We cannot assume that the hierarchical values and desires that are projected onto "we" – *We, the People* with inalienable rights and not *You, the Enslaved* who serve us meals – are simply a thing of the past (Figure 1.2).

Coincidentally, on my way to give a talk – mostly to science, technology, engineering, and mathematics (STEM) students at Harvey Mudd College – that I had planned to kick off with this *Mechanix* ad, I passed two men in the airport restaurant and overheard one say to the other: "I just want someone I can push around …" So simple yet so profound in articulating a dominant and dominating *theory of power* that many more people feel emboldened to state, unvarnished, in the age of Trump. *Push around*? I wondered, in the context of work or dating or any number of interactions. The slavebot, it seems, has a ready market!

For those of us who believe in a more egalitarian notion of power, of collective empowerment without domination, how we imagine our relation to robots offers a mirror for thinking through and against race as technology.

You'll Own

The robots are coming! When they do, you'll command a host of push-button servants.

By O. O. Binder

IN 1863, Abe Lincoln freed the slaves. But by 1965, slavery will be back! We'll all have personal slaves again, only this time we won't fight a Civil War over them. Slavery will be here to stay.

Don't be alarmed. We mean robot "slaves." Let's take a peek into the future

Robots will dress you, comb your hair and serve meals in a jiffy.

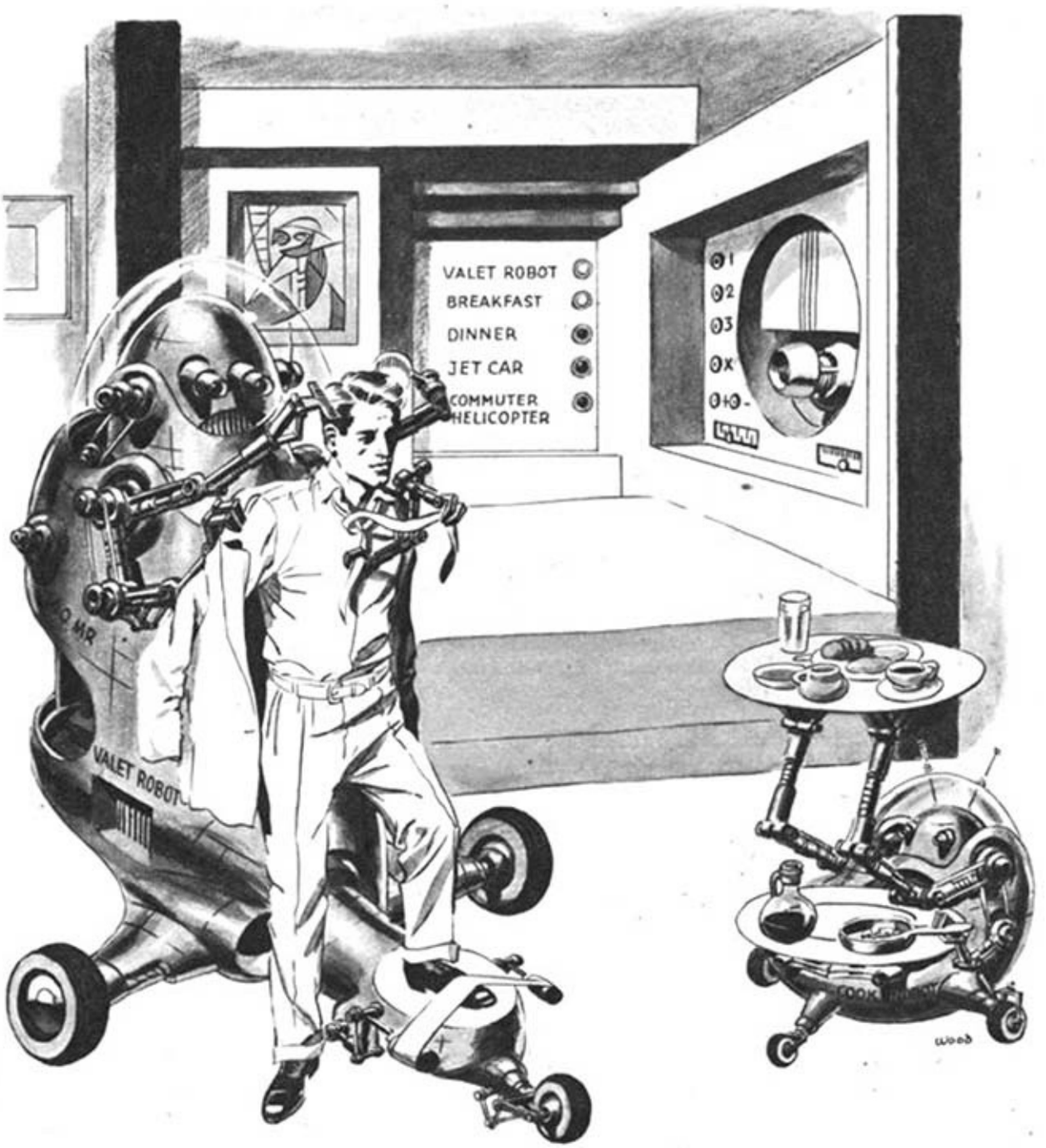


Figure 1.2 Robot Slaves

Source: Binder 1957

It turns out that the disposability of robots and the denigration of racialized populations go hand in hand. We can see this when police officers use "throwbots" – "a lightweight, ruggedized platform that can literally be thrown into position, then remotely controlled from a position of safety" – to collect video and audio surveillance for use by officers. In the words of a member of one of these tactical teams, "[t]he most significant advantage of the throwable robot is that it 'allows them [*sc*. the officers] to own the real estate with their eyes, before they pay for it with their bodies.'"[22] Robots are not the only ones sacrificed on the altar of public safety. So too are the many *Black* victims whose very bodies become the real estate that police officers own in their trigger-happy quest to keep the peace. The intertwining history of machines and slaves, in short, is not simply the stuff of fluff magazine articles.[23]

While many dystopic predictions signal a worry that humans may one day be enslaved by machines, the current reality is that the tech labor force is already deeply unequal across racial and gender lines. Although not the same as the structure of enslavement that serves as an analogy for unfreedom, Silicon Valley's hierarchy consists of the highest-paid creatives and entrepreneurs, who are comprised of White men and a few White women, and the lowest-paid manual laborers – "those cleaning their offices and assembling circuit boards," in other words "immigrants and outsourced labor, often women living in the global south," who usually perform this kind of work.[24] The "diasporic diversity" embodied by South Asian and Asian American tech workforce does not challenge this hierarchy, because they continue to be viewed as a "new digital 'different caste.'" As Nakamura notes, "no amount of work can make them part of the digital economy as 'entrepreneurs' or the 'new economic men.'"[25] Racism, in this way, is a technology that is "built into the tech industry."[26] But how does racism "get inside" and operate through new forms of technology?

To the extent that machine learning relies on large, "naturally occurring" datasets that are rife with racial (and economic and gendered) biases, the raw data that robots are using to learn and make decisions about the world reflect deeply ingrained cultural prejudices and structural hierarchies.[27] Reflecting on the connection between workforce diversity and skewed datasets, one tech company representative noted that, "if the training data is produced by a racist society, it won't matter who is on the team, but the people who are affected should also be on the team."[28] As machines become more "intelligent," that is, as they learn to think more like humans, they are likely to become more racist. But this is not inevitable, so long as we begin to take seriously and address the matter of how racism structures the social and technical components of design.

Raising Robots

So, are robots racist? Not if by "racism" we only mean white hoods and racial slurs.[29] Too

often people assume that racism and other forms of bias must be triggered by an *explicit* intent to harm; for example, linguist John McWhorter argued in *Time* magazine that "[m]achines cannot, themselves, be racists. Even equipped with artificial intelligence, they have neither brains nor intention."[30] But this assumes that self-conscious intention is what makes something racist. Those working in the belly of the tech industry know that this conflation will not hold up to public scrutiny. As one Google representative lamented, "[r]ather than treating malfunctioning algorithms as malfunctioning machines ('classification errors'), we are increasingly treating tech like asshole humans." He went on to propose that "we [programmers] need to stop the machine from behaving like a jerk because it can look like it is being offensive on purpose."[31] If machines are programmed to carry out tasks, both they and their designers are guided by some purpose, that is to say, intention. And in the face of discriminatory effects, if those with the power to design differently choose business as usual, then they are perpetuating a racist system whether or not they are card-carrying members of their local chapter of Black Lives Matter.

Robots are not sentient beings, sure, but racism flourishes well beyond hate-filled hearts.[32] An indifferent insurance adjuster who uses the even more disinterested metric of a credit score to make a seemingly detached calculation may perpetuate historical forms of racism by plugging numbers in, recording risk scores, and "just doing her job." Thinking with Baldwin, someone who insists on his own racial innocence despite all evidence to the contrary "turns himself into a monster."[33] No malice needed, no N-word required, just lack of concern for how the past shapes the present – and, in this case, the US government's explicit intention to concentrate wealth in the hands of White Americans, in the form of housing and economic policies.[34] Detachment in the face of this history ensures its ongoing codification. Let us not forget that databases, just like courtrooms, banks, and emergency rooms, do not contain organic brains. Yet legal codes, financial practices, and medical care often produce deeply racist outcomes.

The intention to harm or exclude may guide some technical design decisions. Yet even when they do, these motivations often stand in tension with aims framed more benevolently. Even police robots who can use lethal force while protecting officers from harm are clothed in the rhetoric of public safety.[35] This is why we must separate "intentionality" from its strictly negative connotation in the context of racist practices, and examine how aiming to "do good" can very well coexist with forms of malice and neglect.[36] In fact a do-gooding ethos often serves as a moral cover for harmful decisions. Still, the view that ill intent is always a feature of racism is common: "No one at Google giggled while intentionally programming its software to mislabel black people."[37] Here McWhorter is referring to photo-tagging software that classified dark-skinned users as "gorillas." Having discovered no bogeyman behind the screen, he dismisses the idea of "racist technology" because that implies "designers and the people who hire them are therefore 'racists.'" But this expectation of individual intent to harm as evidence of racism is one that scholars of race have long rejected.[38]

We could expect a Black programmer, immersed as she is in the same systems of racial meaning and economic expediency as the rest of her co-workers, to code software in a way

that perpetuates racist stereotypes. Or, even if she is aware and desires to intervene, will she be able to exercise the power to do so? Indeed, by focusing mainly on individuals' identities and overlooking the norms and structures of the tech industry, many diversity initiatives offer little more than cosmetic change, demographic percentages on a company pie chart, concealing rather than undoing the racist status quo.[39]

So, can robots – and, by extension, other types of technologies – be racist? Of course they can. Robots, designed in a world drenched in racism, will find it nearly impossible to stay dry. To a certain extent, they learn to speak the coded language of their human parents – not only programmers but all of us online who contribute to "naturally occurring" datasets on which AI learn. Just like diverse programmers, Black and Latinx police officers are known to engage in racial profiling alongside their White colleagues, though they are also the target of harassment in a way their White counterparts are not.[40] One's individual racial identity offers no surefire insulation from the prevailing ideologies.[41] There is no need to identify "giggling programmers" self-consciously seeking to denigrate one particular group as evidence of discriminatory design. Instead, so much of what is routine, reasonable, intuitive, and codified reproduces unjust social arrangements, without ever burning a cross to shine light on the problem.[42]

A representative of Microsoft likened the care they must exercise when they create and sell predictive algorithms to their customers with "giving a puppy to a three-year-old. You can't just deploy it and leave it alone because it will decay over time."[43] Likewise, describing the many controversies that surround AI, a Google representative said: "We are in the uncomfortable birthing stage of artificial intelligence."[44] Zeros and ones, if we are not careful, could deepen the divides between haves and have-nots, between the deserving and the undeserving – rusty value judgments embedded in shiny new systems.

Interestingly, the MIT data scientists interviewed by anthropologist Kathleen Richardson

> were conscious of race, class and gender, and none wanted to reproduce these normative stereotypes in the robots they created … [They] avoided racially marking the "skin" of their creations … preferred to keep their machines genderless, and did not speak in class-marked categories of their robots as "servants" or "workers," but companions, friends and children.[45]

Richardson contrasts her findings to that of anthropologist Stefan Helmreich, whose pioneering study of artificial life in the 1990s depicts researchers as "ignorant of normative models of sex, race, gender and class that are refigured in the computer simulations of artificial life."[46] But perhaps the contrast is overdrawn, given that colorblind, gender-neutral, and class-avoidant approaches to tech development are another avenue for coding inequity. If data scientists do indeed treat their robots like children, as Richardson describes, then I propose a race-conscious approach to parenting artificial life – one that does not feign colorblindness. But where should we start?

Automating Anti-Blackness

As it happens, the term "stereotype" offers a useful entry point for thinking about the default settings of technology and society. It first referred to a practice in the printing trade whereby a solid plate called a "stereo" (from the ancient Greek adjective *stereos*, "firm," "solid") was used to make copies. The duplicate was called a "stereotype."[47] The term evolved; in 1850 it designated an "image perpetuated without change" and in 1922 was taken up in its contemporary iteration, to refer to shorthand attributes and beliefs about different groups. The etymology of this term, which is so prominent in everyday conceptions of racism, urges a more sustained investigation of the interconnections between technical and social systems.

To be sure, the explicit codification of racial stereotypes in computer systems is only one form of discriminatory design. Employers resort to credit scores to decide whether to hire someone, companies use algorithms to tailor online advertisements to prospective customers, judges employ automated risk assessment tools to make sentencing and parole decisions, and public health officials apply digital surveillance techniques to decide which city blocks to focus medical resources. Such programs are able to sift and sort a much larger set of data than their human counterparts, but they may also reproduce long-standing forms of structural inequality and colorblind racism.

And these default settings, once fashioned, take on a life of their own, projecting an allure of objectivity that makes it difficult to hold anyone accountable.[48] Paradoxically, automation is often presented as a solution to human bias – a way to avoid the pitfalls of prejudicial thinking by making decisions on the basis of objective calculations and scores. So, to understand racist robots, we must focus less on their intended uses and more on their actions. Sociologist of technology Zeynep Tufekci describes algorithms as "computational agents who are not alive, but who act in the world."[49] In a different vein, philosopher Donna Haraway's (1991) classic *Simians, Cyborgs and Women* narrates the blurred boundary between organisms and machines, describing how "myth and tool mutually constitute each other."[50] She describes technologies as "frozen moments" that allow us to observe otherwise "fluid social interactions" at work. These "formalizations" are also instruments that enforce meaning – including, I would add, racialized meanings – and thus help construct the social world.[51] Biased bots and all their coded cousins could also help subvert the status quo by exposing and authenticating the existence of systemic inequality and thus by holding up a "black mirror" to society,[52] challenging us humans to come to grips with our deeply held cultural and institutionalized biases.[53]

Consider the simple corrections of our computer systems, where words that signal undue privilege are not legible. The red line tells us that only one of these phenomena, underserved and overserved, is legitimate while the other is a mistake, a myth (Figure 1.3).

But power is, if anything, relational. If someone is experiencing the underside of an unjust system, others, then, are experiencing its upside. If employers are passing up your job application because they associate negative qualities with your name, then there are more

jobs available for more appealing candidates. If, however, we do not have a word to describe these excess jobs, power dynamics are harder to discuss, much less intervene in. If you try this exercise today, your spellcheck is likely to recognize both words, which reminds us that it is possible to change technical systems so that they do not obscure or distort our understanding and experience of social systems. And, while this is a relatively simple update, we must make the same demand of more complex forms of coded inequity and tune into the socially proscribed forms of (in)visibility that structure their design.

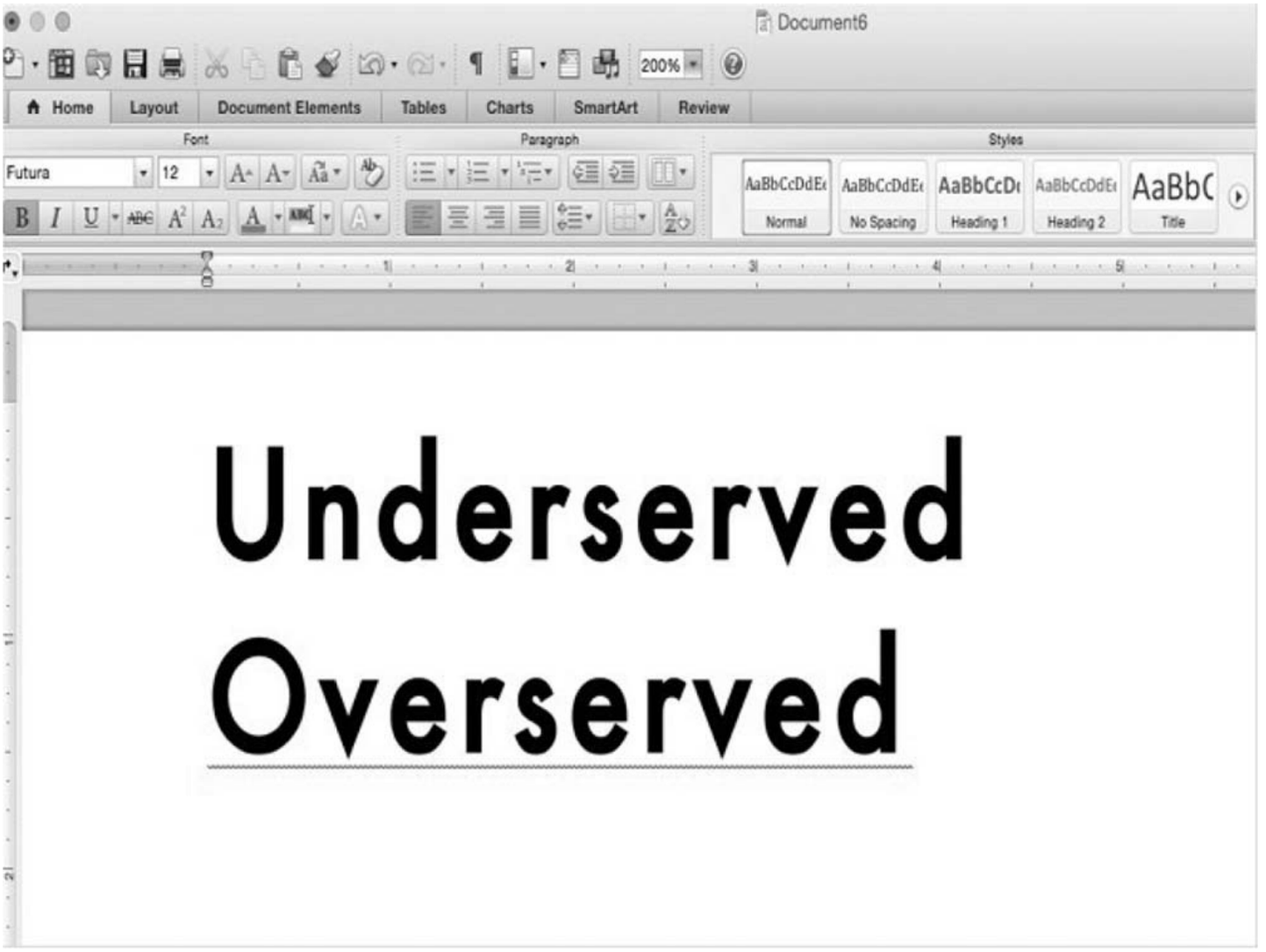


Figure 1.3 Overserved

If we look strictly at the technical features of, say, automated soap dispensers and predictive crime algorithms, we may be tempted to home in on their differences. When we consider the stakes, too, we might dismiss the former as relatively harmless, and even a distraction from the dangers posed by the latter. But rather than starting with these distinctions, perhaps there is something to be gained by putting them in the same frame to tease out possible relationships. For instance, the very idea of hygiene – cleaning one's hands and "cleaning up" a neighborhood – echoes a racialized vocabulary. Like the Beauty AI competition, many advertisements for soap conflate darker skin tones with unattractiveness and more specifically with dirtiness, as did an ad from the 1940s where a White child turns to a Black

child and asks, “Why doesn’t your mama wash you with fairy soap?” Or another one, from 2017, where a Black woman changes into a White woman after using Dove soap. The idea of hygiene, in other words, has been consistently racialized, all the way from marketing to public policy. In fact the most common euphemism for eugenics was “racial hygiene”: ridding the body politic of unwanted populations would be akin to ridding the body of unwanted germs. Nowadays we often associate racial hygienists with the Nazi holocaust, but many early proponents were the American progressives who understood eugenics to work as a social uplift and a form of Americanization. The ancient Greek etymon, *eugeneia* (εὐγένεια), meant “good birth,” and this etymological association should remind us how promises of goodness often hide harmful practices. As Margaret Atwood writes, “Better never means better for everyone … It always means worse, for some.”

Take a seemingly mundane tool for enforcing segregation – separate water fountains – which is now an iconic symbol for the larger system of Jim Crow. In isolation from the broader context of racial classification and political oppression, a “colored” water fountain could be considered trivial, though in many cases the path from segregated public facilities to routine public lynching was not very long. Similarly, it is tempting to view a “Whites only” soap dispenser as a trivial inconvenience. In a viral video of two individuals, White and Black, who show that their hotel soap dispenser does not work for the latter, they are giggling as they expose the problem. But when we situate in a broader racial context what appears to be an innocent oversight, the path from restroom to courtroom might be shorter than we expect.

That said, there is a straightforward explanation when it comes to the soap dispenser: near infrared technology requires light to bounce back from the user and activate the sensor, so skin with more melanin, absorbing as it does more light, does not trigger the sensor. But this strictly technical account says nothing about why this particular sensor mechanism was used, whether there are other options, which recognize a broader spectrum of skin tones, and how this problem was overlooked during development and testing, well before the dispenser was installed. Like segregated water fountains of a previous era, the discriminatory soap dispenser offers a window onto a wider social terrain. As the soap dispenser is, technically, a robot, this discussion helps us consider the racism of robots and the social world in which they are designed.

For instance, we might reflect upon the fact that the infrared technology of an automated soap dispenser treats certain skin tones as normative and upon the reason why this technology renders Black people invisible when they hope to be seen, while other technologies, for example facial recognition for police surveillance, make them hypervisible when they seek privacy. When we draw different technologies into the same frame, the distinction between “trivial” and “consequential” breaks down and we can begin to understand how Blackness can be both marginal and focal to tech development. For this reason I suggest that we hold off on drawing too many bright lines – good versus bad, intended versus unwitting, trivial versus consequential. Sara Wachter-Boettcher, the author of *Technically Wrong*, puts it thus: “If tech companies can’t get the basics right … why should we trust them to provide solutions to massive societal problems?”[54] The issue is not simply that innovation and inequity can go hand in hand but that a view of technology as value-free

means that we are less likely to question the New Jim Code in the same way we would the unjust laws of a previous era, assuming in the process that our hands are clean.

Engineered Inequity

In one of my favorite episodes of the TV show *Black Mirror*, we enter a world structured by an elaborate social credit system that shapes every encounter, from buying a coffee to getting a home loan. Every interaction ends with people awarding points to one another through an app on their phones; but not all the points are created equal. Titled "Nosedive," the episode follows the emotional and social spiral of the main protagonist, Lacie, as she pursues the higher rank she needs in order to qualify for an apartment in a fancy new housing development. When Lacie goes to meet with a points coach to find out her options, he tells her that the only way to increase her rank in such a short time is to get "up votes from quality people. Impress those upscale folks, you'll gain velocity on your arc and there's your boost." Lacie's routine of exchanging five stars with service workers and other "mid- to low-range folks" won't cut it if she wants to improve her score quickly. As the title of the series suggests, *Black Mirror* offers a vivid reflection on the social dimensions of technology – where we *are* and where we might be going with just a few more clicks in the same direction. And, although the racialized dimensions are not often made very explicit, there is a scene toward the beginning of the episode when Lacie notices all her co-workers conspiring to purposely lower the ranking of a Black colleague and forcing him into a subservient position as he tries to win back their esteem … an explicit illustration of the New Jim Code.

When it comes to engineered inequity, there are many different types of "social credit" programs in various phases of prototype and implementation that are used for scoring and ranking populations in ways that reproduce and even amplify existing social hierarchies. Many of these come wrapped in the packaging of progress. And, while the idiom of the New Jim Code draws on the history of racial domination in the United States as a touchstone for technologically mediated injustice, our focus must necessarily reach beyond national borders and trouble the notion that racial discrimination is isolated and limited to one country, when a whole host of cross-cutting social ideologies make that impossible.

Already being implemented, China's social credit system is an exemplar of explicit ranking with far-reaching consequences. What's more, *Black Mirror* is referenced in many of the news reports of China's experiment, which started in 2014, with the State Council announcing its plans to develop a way to score the trustworthiness of citizens. The government system, which will require mandatory enrollment starting from 2020, builds on rating schemes currently used by private companies.

Using proprietary algorithms, these apps track not only financial history, for instance whether someone pays his bills on time or repays her loans, but also many other variables, such as one's educational, work, and criminal history. As they track all one's purchases, donations, and leisure activities, something like too much time spent playing video games marks the person as "idle" (for which points may be docked), whereas an activity like buying diapers

suggests that one is “responsible.” As one observer put it, “the system not only investigates behaviour – it shapes it. It ‘nudges’ citizens away from purchases and behaviours the government does not like.”[55] Most alarmingly (as this relates directly to the New Jim Code), residents of China’s Xinjiang, a predominantly Muslim province, are already being forced to download an app that aims to track “terrorist and illegal content.”

Lest we be tempted to think that engineered inequity is a problem “over there,” just recall Donald Trump’s idea to register all Muslims in the United States on an electronic database – not to mention companies like Facebook, Google, and Instagram, which already collect the type of data employed in China’s social credit system. Facebook has even patented a scoring system, though it hedges when asked whether it will ever develop it further. Even as distinct histories, politics, and social hierarchies shape the specific convergence of innovation and inequity in different contexts, it is common to observe, across this variation, a similar deployment of buzzwords, platitudes, and promises.

What sets China apart (for now) is that all those tracked behaviors are already being rated and folded into a “citizen score” that opens or shuts doors, depending on one’s ranking.[56] People are given low marks for political misdeeds such as “spreading rumors” about government officials, for financial misdeeds such as failing to pay a court fine, or social misdeeds such as spending too much time playing video games. A low score brings on a number of penalties and restrictions, barring people from opportunities such as a job or a mortgage and prohibiting certain purchases, for example plane tickets or train passes.[57] The chief executive of one of the companies that pioneered the scoring system says that it “will ensure that the bad people in society don’t have a place to go, while good people can move freely and without obstruction.”[58]

Indeed, it is not only the desire to move freely, but all the additional privileges that come with a higher score that make it so alluring: faster service, VIP access, no deposits on rentals and hotels – not to mention the admiration of friends and colleagues. Like so many other technological lures, systems that seem to objectively rank people on the basis of merit and things we like, such as trustworthiness, invoke “efficiency” and “progress” as the lingua franca of innovation. China’s policy states: “It will forge a public opinion environment where keeping trust is glorious. It will strengthen sincerity in government affairs, commercial sincerity, social sincerity and the construction of judicial credibility.”[59] In fact, higher scores have become a new status symbol, even as low scorers are a digital underclass who may, we are told, have an opportunity to climb their way out of the algorithmic gutter.

Even the quality of people in one’s network can affect your score – a bizarre scenario that has found its way onto TV shows like *Black Mirror* and *Community*, where even the most fleeting interpersonal interactions produce individual star ratings, thumbs up and down, giving rise to digital elites and subordinates. As Zeynep Tufekci explains, the ubiquitous incitement to “like” content on Facebook is designed to accommodate the desires of marketers and works against the interests of protesters, who want to express dissent by “disliking” particular content.[60] And, no matter how arbitrary or silly the credit (see “meow

meow beenz" in the TV series *Community*), precisely because people and the state invest it with import, the system carries serious consequences for one's quality of life, until finally the pursuit of status spins out of control.

The phenomenon of measuring individuals not only by their behavior but by their networks takes the concept of social capital to a whole new level. In her work on marketplace lenders, sociologist Tamara K. Nopper considers how these companies help produce and rely on what she calls *digital character* – a "profile assessed to make inferences regarding character in terms of credibility, reliability, industriousness, responsibility, morality, and relationship choices."[61] Automated social credit systems make a broader principle of merit-based systems clear: scores assess a person's ability to conform to established definitions of good behavior and valued sociality rather than measuring any intrinsic quality. More importantly, the ideological commitments of dominant groups typically determine what gets awarded credit in the first place, automating social reproduction. This implicates not only race and ethnicity; depending on the fault lines of a given society, merit systems also codify class, caste, sex, gender, religion, and disability oppression (among other factors). The point is that multiple axes of domination typically converge in a single code.

Take the credit associated with the aforementioned categories of playing video games and buying diapers. There are many ways to parse the values embedded in the distinction between the "idle" and the "responsible" citizen so that it lowers the scores of gamers and increases the scores of diaper changers. There is the ableist logic, which labels people who spend a lot of time at home as "unproductive," whether they play video games or deal with a chronic illness; the conflation of economic productivity and upright citizenship is ubiquitous across many societies.

Consider, too, how gender norms are encoded in the value accorded to buying diapers, together with the presumption that parenthood varnishes (and, by extension, childlessness tarnishes) one's character. But one may wonder about the consequences of purchasing too many diapers. Does reproductive excess lower one's credit? Do assumptions about sex and morality, often fashioned by racist and classist views, shape the interpretation of having children and of purchasing diapers? In the United States, for instance, one could imagine the eugenic sensibility that stigmatizes Black women's fertility and celebrates White women's fecundity getting codified through a system that awards points for diapers purchased in suburban zip codes and deducts points for the same item when purchased in not yet gentrified parts of the city – the geography of social worth serving as a proxy for gendered racism and the New Jim Code. In these various scenarios, top-down reproductive policies could give way to a social credit system in which the consequences of low scores are so far-reaching that they could serve as a veritable digital birth control.

In a particularly poignant exchange toward the end of the "Nosedive" episode, Lacie is hitchhiking her way to win the approval of an elite group of acquaintances; and motorists repeatedly pass her by on account of her low status. Even though she knows the reason for being disregarded, when a truck driver of even lower rank kindly offers to give her a ride, Lacie looks down her nose at the woman ("nosedive" indeed). She soon learns that the driver

has purposefully opted out of the coercive point system and, as they make small talk, the trucker says that people assume that, with such a low rank, she must be an "antisocial maniac." Lacie reassures the woman by saying you "seem normal." Finally, the trucker wonders about Lacie's fate: "I mean you're a 2.8 but you don't *look* 2.8." This moment is illuminating as to how abstract quantification gets embodied – that the difference between a 2.8 and a 4.0 kind of person should be self-evident and readable on the (sur)face. This is a key feature of racialization: we take arbitrary qualities (say, social score, or skin color), imbue them with cultural importance, and then act as if they reflected natural qualities in people (and differences between them) that should be obvious just by looking at someone.[62]

In this way speculative fiction offers us a canvas for thinking about the racial vision that we take for granted in our day-to-day lives. The White protagonist, in this case, is barred from housing, transportation, and relationships – a fictional experience that mirrors the forms of ethno-racial exclusions that many groups have actually experienced; and Lacie's low status, just like that of her real-life counterparts, is attributed to some intrinsic quality of her person rather than to the coded inequity that structures her social universe. The app, in this story, builds upon an already existing racial arithmetic, expanding the terms of exclusion to those whose Whiteness once sheltered them from harm. This is the subtext of so much science fiction: the anxiety that, if "we" keep going down this ruinous road, then *we might be next*.

Ultimately the danger of the New Jim Code positioning is that existing social biases are reinforced – yes. But new methods of social control are produced as well. Does this mean that every form of technological prediction or personalization has racist effects? Not necessarily. It means that, whenever we hear the promises of tech being extolled, our antennae should pop up to question what all that hype of "better, faster, fairer" might be hiding and making us ignore. And, when bias and inequity come to light, "lack of intention" to harm is not a viable alibi. One cannot reap the reward when things go right but downplay responsibility when they go wrong.

Notes

1. Visit Beauty.AI First Beauty Contest Judged by Robots, at http://beauty.ai.

2. Pearson 2016b.

3. Pearson 2016b.

4. Levin 2016.

5. Both Harcourt quotations are from Levin 2016.

6. See http://beauty.ai.

7. See https://machinelearningmastery.com/what-is-deep-learning.

8. Metz 2013.

9. Field note, Jack Clark's Keynote Address at the Princeton University AI and Ethics Conference, March 10, 2018.

10. The flip side of personalization is what Eubanks (2018) refers to as an "empathy override." See also Edes 2018.

11. Fox 2012, n.p.

12. "Homelessness is not a systems engineering problem, it's a carpentry problem" (Eubanks 2018, p. 125).

13. The term "uncanny valley" was coined by Masahiro Mori in 1970 and translated into English by Reichardt (1978).

14. But it is worth keeping in mind that many things dubbed "AI" today are, basically, just statistical predictions rebranded in the age of big data – an artificial makeover that engenders more trust as a result. This point was made by Arvind Narayanan in response to a Microsoft case study at a workshop sponsored by the Princeton University Center for Human Values and Center for Informational Technology Policy, October 6, 2017.

15. Truitt 2016.

16. Richardson 2015, p. 5.

17. Richardson 2015, p. 2.

18. As Imani Perry (2018, p. 49) explains, "Mary Shelley's *Frankenstein* provided a literary example of the domestic anxiety regarding slavery and colonialism that resulted from this structure of relations … Frankenstein's monster represented the fear of the monstrous products that threatened to flow from the peculiar institutions. The novel lends itself to being read as a response to slave revolts across the Atlantic world. But it can also be read as simply part of anxiety attendant to a brutal and intimate domination, one in which the impenetrability of the enslaved was already threatening."

19. Richardson 2015, p. 2.

20. Everett 2009, p. 1.

21. Binder 1957.

22. These passages come from a PoliceOne report that cautions us: "as wonderful an asset as they are, they cannot provide a complete picture. The camera eye can only see so much, and there are many critical elements of information that may go undiscovered or unrecognized … Throwable robots provide such an advance in situational awareness that it can be easy to forget that our understanding of the situation is still incomplete" (visit https://www.policeone.com/police-products/police-technology/robots/articles/320406006–5-tactical-considerations-for-throwable-robot-deployment).

23. Rorty 1962.

24. Daniels 2015, p. 1379. See also Crain et al. 2016; Gajjala 2004; Hossfeld 1990; Pitti 2004; Shih 2006.

25. Nakamura 2002, p. 24.

26. Daniels 2013, p. 679.

27. Noble and Tynes 2016.

28. Field note from the Princeton University Center for Human Values and Center for Informational Technology Policy Workshop, October 6, 2017.

29. The notion of "racist robots" is typically employed in popular discourse around AI. I use it as a rhetorical device to open up a discussion about a range of contemporary technologies, most of which are not human-like automata of the kind depicted in films and novels. They include forms of automation integrated in everyday life, like soap dispensers and search engines, bureaucratic interventions that seek to make work more efficient, as in policing and healthcare, and fantastical innovations first imagined in science fiction, such as self-driving cars and crime prediction techniques.

30. McWhorter 2016.

31. Field note from the Princeton University Center for Human Values and Center for Informational Technology Policy Workshop, October 6, 2017.

32. The famed android Lieutenant Commander Data of the hit series *Star Trek* understood well the distinction between inputs and outputs, intent and action. When a roughish captain of a small cargo ship inquired whether Data had ever experienced love, Data responded, "The act or the emotion?" And when the captain replied that they're both the same, Data rejoined, "I believe that statement to be inaccurate, sir." Just as loving behavior does not require gushing Valentine's Day sentiment, so too can discriminatory action be fueled by indifference and disregard, and even by good intention, more than by flaming hatred.

33. Baldwin 1998, p. 129.

34. See https://www.nclc.org/images/pdf/credit_discrimination/InsuranceScoringWhitePaper.pdf.

35. Policeone.com, at https://www.policeone.com/police-products/police-technology/robots.

36. This is brought to life in the 2016 HBO series *Silicon Valley*, which follows a young Steve Jobs type of character, in a parody of the tech industry. In a segment at TechCrunch, a conference where start-up companies present their proof of concept to attract venture capital investment, one presenter after another exclaims, "we're making the world a better place" with each new product that also claims to "revolutionize" some corner of the

industry. See https://longreads.com/2016/06/13/silicon-valley-masterfully skewers-tech-culture.

37. McWhorter 2016.

38. Sociologist Eduardo Bonilla-Silva (2006) argues that, “if racism is systemic, this view of ‘good’ and ‘bad’ whites distorts reality” (p. 132). He quotes Albert Memmi saying: “There is a strange enigma associated with the problem of racism. No one, or almost no one, wishes to see themselves as racist; still, racism persists, real and tenacious” (Bonilla-Silva 2006, p. 1).

39. Dobush 2016.

40. Perry explains how racial surveillance does not require a “bogeyman behind the curtain; it is a practice that emerges from our history, conflicts, the interests of capital, and political expediency in the nation and the world … Nowhere is the diffuse and individuated nature of this practice more apparent than in the fact that over-policing is not limited to White officers but is instead systemic” (Perry 2011, p. 105).

41. Calling for a post-intentional analysis of racism, Perry argues that intent is not a good measure of discrimination because it “creates a line of distinction between ‘racist’ and ‘acceptable’ that is deceptively clear in the midst of a landscape that is, generally speaking, quite unclear about what racism and racial bias are, who [or what] is engaging in racist behaviors, and how they are doing so” (Perry 2011, p. 21).

42. Schonbrun 2017.

43. Field note from the Princeton University Center for Human Values and Center for Informational Technology Policy Workshop, October 6, 2017.

44. Field note from the Princeton University Center for Human Values and Center for Informational Technology Policy Workshop, October 6, 2017.

45. Richardson 2015, p. 12.

46. Richardson 2015, p. 12; see also Helmreich 1998.

47. See s.v. “stereotype” at https://www.etymonline.com/ word/stereotype (Online Etymology Dictionary).

48. “It is to say, though, that all those inhabiting subject positions of racial power and domination – notably those who are racially White in its various formulations in different racially articulated societies – project and extend racist socialities by default. But the default is not the only position to occupy or in which to invest. One remains with the default because it is given, the easier to inhabit, the sociality of thoughtlessness” (Goldberg 2015, pp. 159–60).

49. Tufekci 2015, p. 207.

50. Haraway 1991, p. 164.

51. Haraway 1991, p. 164.

52. This potential explains the name of the provocative TV series *Black Mirror*.

53. According to Feagin and Elias (2013, p. 936), systemic racism refers to "the foundational, large-scale and inescapable hierarchical system of US racial oppression devised and maintained by whites and directed at people of colour … [It] is foundational to and engineered into its major institutions and organizations."

54. Wachter-Boettcher 2017, p. 200. On the same page, the author also argues that "[w]e'll only be successful in ridding tech of excesses and oversights if we first embrace a new way of seeing the digital tools we rely on – not as a wonder, or even as a villain, but rather as a series of choices that designers and technologists have made. Many of them small: what a button says, where a data set comes from. But each of these choices reinforces beliefs about the world, and the people in it."

55. Botsman 2017.

56. Nguyen 2016.

57. Morris 2018.

58. State Council 2014.

59. State Council 2014.

60. Tufekci 2017, p. 128.

61. Nopper 2019, p. 170.

62. Hacking 2007.

sonix

NAME
casteist-tech.mp3

DATE
February 16, 2023

DURATION
49m 34s

5 SPEAKERS
Speaker1
Speaker2
Speaker3
Speaker4
Speaker5

START OF TRANSCRIPT

[00:00:17] Speaker1
Welcome to Radical A.I., a podcast about technology, power society and what it means to be human in the age of information. Today, we have a special surprise for all of you. Your typical hosts, Gests myself and Dylan will not be conducting the interview in this episode. We have a special surprise host instead. If you've been following along with our podcast and organization for a while, you might remember that over the last six months we've been running a radical AI podcast internship with two amazing interns, Nikil Dhanraj and Lena Wang. And both of these interns have been working hard over the last six months on several projects, including a series of roundtable dinner discussions about radical visions for technology, which was led by our intern Nikil, and also in collaboration with the White House Foundation and an entire curriculum and set of resources on technology and power, which was led by our intern, Lena. We were so happy to see so many of you at the roundtable events that were led by Nikil over the last few months. And be sure to stay tuned for more information about Leena's projects and curriculum in the coming months as they're launched. And speaking of the incredible work that these interns have done over the last few months. Today is a bittersweet day because today marks the final day of the riots, 21 spring internship. In order to mark the celebration, we are releasing our very first interview conducted by a guest host, one of our interns, Nikil Demiraj. So in this episode, Nikil speaks to 10 Modisane Androgen and Seema Hardy about technology, casteism and surveillance. Dunwoodie is a Dalit rights artist, technologist and theorist. Currently then, Modi is the co-founder and executive director of Equality Labs. CEMA is an engineer and an anti caste and anti colorism activist. And now we'll hand it over to Nikil to take it from here.

[00:02:26] Speaker2
Hi, all, welcome back to another episode of the Radical Eye podcast, so excited to be joining you all today with two incredible guests on the show, Seema Hari and then Morris in the region. And today we're going to be having a very important and fruitful conversation about caste technology and surveillance. So thank you so much and welcome to Seema. And then. So to go ahead and kick off this conversation, I wanted to start by asking you all, how can we conceptualize networks of caste and the production of technology both in South Asia and the South Asian diaspora? And maybe as we go through this conversation, also for our listeners who don't know, it would be great to sort of give a working definition and understanding of caste frameworks in general.

[00:03:08] Speaker3
So I think that this is such an interesting question, because I think that this has been the heart of the work that equality that has been working on for the last five years is really talking about the ways that we're seeing caste apartheid reorganize itself within the digital space. And when you think about the work that Professor Noble has done to really illuminate how structural bias is embedded in code and embedded in supply chains and embedded into workplaces, those are all of the ways that we're seeing caste be we organized in digital realms. And this is something that I often talk about in terms of the theoretical work that we do around test and tech bias as digital ism, where you're basically seeing the logics of caste, you know, not only be transported, but really become the underpinning of so much of the digital infrastructure, both for South Asia and South Asian tech talent that might travel as part of these global supply chains for all of these conglomerates. And the ways that we see caste show up are profound. You know, we are seeing it in terms of caste as hostile workplaces where we see caste oppressed workers seeing slurs and harassment and discrimination become normalized by, you know, in workplaces where even they know that this is a problem they don't have, are properly trained to identify and arrest some of these conditions. We are also seeing this in terms of data stewardship.

[00:04:53] Speaker3
And when we think of, you know, surveillance capitalism, I think that in the South Asian context, this is a surveillance capitalism, not emboldened just by white supremacy, but a white supremacist and rabbinical framework around millions of Dalit and other caste oppressed bodies and communities and geographies. And I also think that we are seeing widespread disinformation networks that are primarily dominant caste networks, who are emboldened by companies who are not implementing their own guidelines to protect and do their basic duty of care with our with within the South Asian markets, but also quite critically, are allowing the normalization of caste system, religious slurs. So the ecosystem for bias and discrimination and the digitization of caste apartheid is in so many realms. And and I think that you can't just speak to it about it being one element, one thing. It is the way that all systems of oppression work. These, you know, techno utopian outlooks that CEOs might pitch to venture capitalists is not the material reality of how these technologies get brutally implemented and hundreds of millions of users and the bias that's baked in, you know, perpetuates and creates even more divides. And so our challenge as technologists who care about caste and racial and gender equity is that we need to basically have an analysis that helps us understand what is broken about these systems and then work forward to kind of address the challenges from that place.

[00:06:47] Speaker4
Yeah, I absolutely agree, and then he really did a good job at explaining the macro effects of all of this, and I really think coming from it in coming from the tech industry, for me, the way that it scares me the most is how technology is really brutal in its analysis. Right. Like whenever you're making a decision as a human being, there's a lot of nuance of world. But as soon as you bring tech into those decisions and like the way describe when you have all these tech European CEOs who are saying that, hey, where are you going to use algorithms to solve everything? Well, algorithms based are based on one and zero decisions, like a string of one and zero decisions. And a lot of these things cannot be cannot be categorized as one zero decisions. And because of that, what you see happening is that algorithms are actually increasing the divide, I would say, and increasing the digital divide and the socio economic divide and contributing in ways that are more harmful than when humans would make those decisions, I would argue. So for me, it's really just like thinking about, you know, when we're talking about straight from like the production of technology, like even, you know, when you think about how people are hired now, that is based on algorithms. Right. So you might you know, LinkedIn is running a machine learning algorithm, box office of candidates for you. But how do you know that the algorithm is not biased against Lucas and gossipers people? Because they might be the ones who never get hired eventually. So then, you know, like and they might not be the ones who are picked in these pools in the first place.

[00:08:18] Speaker4
So that's what scares me the most. And, you know, I that that influenzae I don't know I don't even know the answers to like, how do you combat that? I feel like we need we a digital researchers and people who are writing these algorithms to consider all these factors in their training algorithms, etc., and, you know, like the end result in, you know, there are so many technology workers that are coming from Indian institutes and coming in for their master's degrees as well. And because of the lack of cost reduction and the lack of protection against discrimination for gossipers, folks, we are kind of at the mercy of of managers and professors, et cetera, to protect us. And there's nothing else protecting us. And it prevents us from speaking up even if something happens. You are you are so afraid to speak up because there's no protection. And the second thing is that you risk losing your visa or your job, which then sends you back to where you came from. And, you know, you might have actually escaped a lot of, like, negative experiences or you might be escaping something from your home country. So there's a lot of things in play. And I feel like algorithms and technology are actually emboldening people and building the discrimination that's happening. So we really need to look at it from the from the point of view of empowering the researchers and the engineers who are making these algorithms to be educated at the very least, at the most basic level about what cost means and how it manifests in in social groups.

[00:09:55] Speaker2
Absolutely. Thank you both so much for those incredibly illuminating answers and the frameworks you both laid out make a ton of sense. One thing I wanted to zone in on a little bit is I know that more. You mentioned the term cost apartheid. Would you be able to provide a definition or framework for those listeners who might not be familiar with caste apartheid as a concept?

[00:10:17] Speaker3
Sure. And it's so funny because I think sometimes we're in the middle of of work that you've done for a long time. You forget that you have to take a bird's eye view, you know, particularly because I think that in the United States, though, we have such a great concentration of technical companies. You know, most folks actually lack basic competencies as to what caste is. So just to give people, you know, a basic framework, caste is a system of oppression, analogous, but not the same as race. And I think like race, it is a social fiction. There is no biological foundation to caste. But, you know, the premise of caste is that it was set up in its origins in scripture. And the idea is that, you know, Brahmins who were the priests who developed this system basically carved up the rest of society such that as people, you know, you go down the pyramid, you get more and more polluted because you have less and less desirable jobs. So, you know, the the top is the Brahmins, who are the folks who focus on knowledge and spiritual practices and ritual and kind of hold the the container around what is considered divine and pure and basically get to write the spiritual paradigm. Underneath that, you have the Qataris who are the rulers.

[00:11:47] Speaker3
And then you have the bishops who are the merchants and then you have a peasant caste that's called the shudders, and outside of that system is a group of people that were considered so outcast that they were untouchable because they were spiritually defiling. And, you know, communities that were seen as untouchable, faced punishing violence, extreme social exclusion, which is one of the reasons why we use the term caste apartheid, because essentially where you land on this system can determine who you marry, what job you have, what side you will live on, whether you have access to water and your proximity to violence and structural privileges or lack thereof. And for many that were untouchable, I mean, this was just a grueling sentencing, violent experience, you know. And, you know, I think part of that resistance was that people were like, we don't we don't want to call ourselves untouchable. That's an epithet. So we use the term Dalit. And so, you know, within that little mini history lesson for anyone that is in the tech field and not someone who spends a lot of time in the social sciences, I want to really kind of emphasize you don't need to be a history major to understand that violations, of course, are civil rights violations and all of the things that you would understand better violations for protected classes of people like race and gender and sexual orientation are exactly the same things that you're hearing from from people who are caste oppressed, you know, from slurs in the workplace, discrimination and harassment, terminal termination, termination.

[00:13:32] Speaker3
You know, it's all very practical in terms of how you would look at this from a DCI framework. So I don't think that you need to to know the entire history of it, thousands of years of the caste system to know that it's a problem, that we're seeing caste bias rampant across all aspects of tech and it needs to be addressed meaningfully. And it starts by adding caste as a protected category, which opens the door to data collection and opens the door for open and transparent conversations about the kinds of discrimination that might be happening inside your company, as well as positive investments in terms of coaching and apprenticeships and recruitment and and having suppressed employees not only feel safe about coming out in their workplaces, but actually being able to feel confident in going up there. The, you know, the success pipeline of a particular company. And this is a big deal, because when you think about the amount of South Asians that work in the tech field and that India is a market that most companies want to basically conquer, you know, it's not just the moral thing to do.

[00:14:44] Speaker3
It's actually great business sense because the growth of the Indian market is with the next billion users who are all, you know, majority caste oppressed peoples because they are the last to get online. So it makes sense to have a diverse workspace that can actually speak to those users and really move them into places of confidence and and tooling and creating content that really speaks to this moment. So, you know, it's it's a really important moment that I want to encourage anyone within the tech field that's listening to this podcast to consider, you know, it's great business sense. You're on the right side of history. And more important, you'll be compliant with lock. His caste discrimination is legal and the amount of caste discrimination that we're seeing is so wild, it would really do many of the companies that are listening to consider that they don't be the next Cisco. They're not the next company that's sued by a state for caste discrimination because they didn't take the bull by its horns and really work on it proactively as opposed to through litigation.

[00:15:51] Speaker4
Absolutely, and I think I really I agree with everything that moves that I really want to underscore the point about reaching the next next frontier in India, about reaching all the users who are just starting to come online, etc.. I think I see that a lot in the tech industry. And the biggest problem is that people are looking at it from the lens of people who are sitting in the Silicon Valley. So they're like, oh, we need to build an app for this. And I've been in so many situations where I've been able to explain to them that, you know, these are my people. They don't have feature. They have feature phones. They don't have phones with androids on them. I mean, now they do. But earlier they didn't even have that. But people are thinking of creating solutions that were centered around Android apps. So you need that person in the room to help you think about human centered design. Right. And, you know, we have all these Silicon Valley technologies, UX researchers, you researchers talking about human centered design, but they don't have any decision makers who understand the nuance of the people on the ground and the people who will, you know, eventually use their apps. So I really believe in increasing that representation. I think the representation is something really low. I don't even think we have done enough data collection to understand what the representation of gossipers groups is within the huge technology force in America that comes from India. But I think that number is really low and it all big. It all starts with acknowledging that this is a problem and then taking the steps that Nimoy's just laid out where you make Gosta protected category and then people are comfortable about disclosing their costs and then providing positive reinforcement and positive upliftment opportunities for those people.

[00:17:29] Speaker2
Yeah, absolutely. Thank you so much for those frameworks. Those are incredibly useful to keep in mind and really, really relevant to the current moment. I know also that in this conversation, the Cisco case came up and I'm curious to, I guess, learn a little more about that and then also think about the term you suggested that Morri Digital Romanism, how can we understand the digital Romanism and how it manifests not just in the culture of these workplaces, like with the Cisco case, but also in the products of technology themselves?

[00:18:00] Speaker3
So I think what's so important with the Cisco case is that, you know, as we're looking at, you know, landmarks in terms of American institutions really being forced to confront how big of a problem cast is. I think the State of California's Department Fairness in Employment and Housing, suing Cisco is a pretty big one, because what the DFJ did essentially was investigate, you know, the the complainant who's described pretty horrific experiences, which included, you know, aggressive kind of intimidation and harassment. And DFI doesn't take it lightly. You know, a case like this, they're actually very clear before they investigate, you know, that they're not going to pursue every complaint. But the fact that they were able to do this really shows that they believe that the case has deep merit and they're going to pursue the litigation all the way to the end. And these cases like, you know, will last many years. So it's not an insignificant amount of resources. And it's a bellwether, I think, in terms of American institutions understanding. It is time that we addressed cast. And, you know, and I think that, you know, this is also a bellwether for the whole sector, because I think it was because of BIPAC scholars like Sophia Noble or the folks behind the Algorithmic Justice Project that we are having critical interventions in terms of the development of A.I., in terms of the people who are stewards of our data under surveillance capitalism, because the communities that are being surveilled are not anywhere near the stewardship or design of these conversations.

[00:19:44] Speaker3
And I think with digital is I mean, unfortunately, it's the same thing, you know, in terms of caste depressed communities. And and I think what's important is that we stop building tech without intention and we need to start thinking about what are the blueprints for our liberation and then build technology that serves in that capacity. Because right now we have technology that basically serves venture capital pipelines that have no human rights impact assessments. So when they get deployed in our markets and on our bodies and on our data, you know, they have immeasurable ways that they are causing harm. And there is no easy remedy because once you kind of crack that egg, there's nothing else people can imagine. You know, it's too big to fail. What are we supposed to do? Well, you know, and I think we have to do better than that, particularly coming into this moment. And covid we have a responsibility that what comes next doesn't create conditions that could harm us in the future. And so. I think that's really what I'm most concerned about right now

[00:20:54] Speaker4
And to the second part of your question, Nicole, I do see this manifesting in technology products as well. You know, the first example that I gave was algorithms, but there's also like features that you see online that you're like, why has this been designed in a very romantic lens? You know, like, for example, on Indian marriage websites, you can filter by cost. You could even filter by skin color at a certain point. And there was a lot of, you know, organizing around that and they removed the skin color photo. But you're still allowing people to organize by these old traditional ideas of cost base and. Right. So, you know, there's a lot of mako's of this even like in technological products themselves. And that's I believe that's because the engineers who are building this are mostly from Casterbridge backgrounds and they think this is just a normal thing that they have to do under the name of tradition and. Right. And so they haven't really looked at it from any other lens whatsoever. So it's not you know, I think that it goes beyond just workplace dynamics. It's in the products all around us. For example, on Instagram, too, there was an account called Buffalo Intellectual who did an analysis of how many of cost activists are verified, like none of us get verified because, you know, Instagram people who decide the verification, you know, who have the decision making capability of who gets verified, they are probably from a predominately cosmopolitan.

[00:22:22] Speaker4
And so they don't believe that, you know, these people need to get verified or whatever that algorithm is deciding at the end. So I see this manifesting a lot in technological products themselves. And, you know, I feel like there is no person in the room who is capable of making these decisions. And that's why we are seeing all of this. But like then, we said, we have to build that line really stuck with me. Actually, we have to build for our bright future. So we build backwards from that to say like what we want to see in the future for our liberation and then build backwards from that instead of having these, like, really data products that we fix, you know, keep on fixing, but it never really gets better. So, yeah, that thank you family for that line. That will stick with me forever.

[00:23:08] Speaker3
And I do think it's important that we need to be ambitious for what we want. I honestly, I am not interested in creating a research complex that's all about let's fix shitty tech, you know, and you know and research at our own cost while our people are dying, because that's literally what's happening. Our people are dying. Why this crap is happening. Like, if you just think about the violence that disinformation networks have done in India, not just South Asia and India alone, think about the chaos. You know, I was just talking to a Muslim friend who lost 30 members of her family to covid 30 members. And the death started, you know, early in the pandemic, because if you remember, there was disinformation that was being pushed, called Korona Jihad that was targeting Indian Muslims. And as a result, throughout the entire pandemic, Indian Muslims were denied medical care from multiple institutions. This is fucking criminal. And, you know, the bananas thing is, is like when you take a company like Facebook, they are so negligent, absolutely unequal, you know, and they are just negligent, you know, from the fact that they had to fire one of their top racist who quote unquote, resigned. But we all know what it was because of her political biases, but also that they have said that they are afraid to remove groups that are extremist in nature because they are afraid of what would happen to their staff and their offices. So what they're essentially saying is that it's unsafe for us to moderate and maintain the guidelines and, oh, well, you know, to basically hundreds of millions of Indian users. But I would ask the question, if you find it on safety, even, you know, moderate in the country, then what business do you two have even been in the country doing business in the first place? And we're not asking these questions because, again, of the colonial and terminable dynamics at play with these companies, you know, the fact that you have a colonial administrator in Silicon Valley that works with dominant caste people to basically allow hate speech to become normalised, disinformation to run rampant, you know, calls for violence to occur and without consequences.

[00:25:31] Speaker3
That is the danger of digital pragmatism. And I want to make very clear, having an analysis around Brahmin ism isn't about targeting one caste. It's about the system that creates. Part died, and that is so really critical because, you know, when you think about talking about nante blackness, you know, the the the the consequences of race are held on black and brown bodies and indigenous bodies. But there was a very clear ideology that set up white folks and created a social fiction so to with Romanism. And we can't shy away from using the term Romanism. Familiar with it because it is the tool for understanding the supremacist system. So I would just like really want to emphasize how critical it is for us to use the right terminology, because when we can accurately diagnose the problem, we can find the best medicine. But when we're kind of in the margins, like hunting for the right terms, we're just clawing around trauma and clawing around the consequences without accuracy to be able to design for it. And there are many, many tools that we can use right now to design for this, but only for being really conscious about our next steps.

[00:26:48] Speaker2
Yeah. Thank you so much for those incredible answers. And I think that what you all have described as digital traumatism is such an important framework to keep in mind. And it sort of leads me into my next question, which is I'm curious about how we can understand digital Romanism in a longer history, where Brauman appropriation of knowledge has been like a very important focal point of outcaste scholarship. How do we understand digital Romanism and situated in that history?

[00:27:18] Speaker3
Well, I mean, for me, because, again, this is like a body of work that I've been developing. And so, you know, I think that if you go back to your book on slavery, he that is like one of the kind of polemical texts that really outlines the crimes of Brahmin isms and the ways that it is enslaved the caste oppressed masses. So when you start with that articulation of Brahmin ism, that actually goes very deeply into the bureaucratic mechanisms of caste and how, you know, the top caste kind of manipulate like the other caste professions in order to maintain their power and the ways that they connect up with the English. There is a direct through line from Fullam to Ambedkar to iodized to BTR to current thinking in terms of caste and its digital forms, which I think are actually very crucial for us to be able to root ourselves in. Because we do have language, we do have foundation and the ideological understanding of the system. What we need to do is frame it in the context of how do we understand bias to work in tech? And it happens in terms of the places where people get developed as technologies so that it's it happens in the context of workplaces and hostile workplaces. It happens in terms of the iteration of the priorities of a market or the design of a particular product. You know, it happens in terms of who defines it, that data set and who is a carceral body to be framed within those contexts. Right. And then I also think it has to do with the way data is controlled and the way that data is weaponized and who gets to make the parameters of that from a stewardship perspective. So those are all really key places where we will see opportunities for there to be research and dialogue and discourse. But this moment around digital Brahmin ism is so severe because of all the consequences that are coming out of it right now.

[00:29:23] Speaker4
Yeah, and for me, it's also about like the people who are in positions of power and who are, you know, releasing the information. I mean, you know, kind of these words of curation of what gets out to the general public are the ones who, you know, are from privileged backgrounds. So you will see this in like not just tech, but also in storytelling, et cetera, where the decision makers have get to tell the stories are from Kasparov's backgrounds. So, you know, the knowledge that they are willing to disclose is the one that protects them as well. So you see this a lot when like, you know, when filmmakers are making movies about any Antigua's movement, they are referencing either Gandhi or some other Rummenigge leader and not Ambedkar, who was the champion for our civil rights. Right. So you see that same thing? I think even in research and everywhere else where you might have junior researchers who are contributing to people, but ultimately the people who are releasing the information and the people who are doing the research are majority in majority from privileged backgrounds. And the same thing happens with tech as well. So, you know, you might you can fight an internal battle to make an algorithm better. But ultimately, it's the head of Facebook who is going to make a decision about how algorithms are controlled in India and how they can make really easy tools for the South to use for the governments to use, but not easy tools for human beings to report this information and human beings to report against, you know, harassment and bullying because, you know, how easy is it for, you know, Instagram or Facebook to put another category in, like, hey, I'm getting bullied and this person is using this. It's not against me or any of those kind of rules in place. But they don't do it because they're decision makers for. I'm from these gospel backgrounds, and they don't want this to come to the forefront. So, yeah, I, I just wanted to add that is

[00:31:18] Speaker2
One thing that also, you know, a lot of the scholarship that you all have been referencing regarding highlighting structural bias and structural violence as it pertains to technology, has also been around surveillance. And so I'm really interested to hear your thoughts on making sense of cost as a social variable when we are studying and understanding surveillance, particularly given the moment right now in India with the rise of Hindu fascism.

[00:31:44] Speaker3
So I think that, you know, one of the things I think that's so important for people to know is that Dalit and caste oppressed peoples are one of the most caste realized communities in the global context, and that we have faced caste morality in every aspect of our lives. And it gets translated into structures of policing and surveillance very easily. And, you know, I'm really remembering like. You know, the you know, and for folks that don't even know, like last year, you know, before the pandemic hit, you know, India was in a genocidal crisis where they were about to create one of the largest networks of, you know, detention camps to target Muslims and caste oppressed peoples. And there's an entire data infrastructure that would be part of that. So at a very real material level, tech would be weaponized by people who would use these data sets to find people, denaturalized them and put them into jail and begin the process of what it means to really enact genocide. And I think this is a very critical thing to look at because it's both about the tech that is used to cast realize, you know, whether it's the use of like CCTV and other kinds of monitoring that happens. But also, there were several instances last year in wide scale protests where the Indian government was identifying people through facial recognition and was open about doing that.

[00:33:23] Speaker3
And and I also think that we are seeing, you know, a large scale collaboration of American platforms with a genocidal administration. And I think we have to ask ourselves, what does this mean? You know, when you think about IBM and its role in the Holocaust, you know, there should be a response from American corporations about never again. So what are the ethics of operating in a genocidal context and what level of transparency and oversight is required so that there isn't a harm that is done to vulnerable human rights defenders? And this is super important because just a couple of months ago, Google participated with, you know, the Delhi Central Police to remand, you know, a young activist who had shared a toolkit about the farmers protest, which was a set of protests related to Punjabi farmers who were striking against what they viewed as very unjust. And they are very unjust revisions to farmers law. And the response was draconian. And, you know, so, too, was the use of surveillance, where they basically asked Google to divulge the IP addresses of everyone that opened up this Google doc. And then that gave the Delhi police like a list of people to come in and remand, which means to kidnap them in the middle of the night, not let their parents know, not give them legal support and to put them into conversation with the police.

[00:34:58] Speaker3
Why did you do that? Remember when Google was like, do no evil? This seems like the opposite of like, let's absolutely not just collaborate but be complicit with evil. Straight up, you know, and you can't tell me that they don't know what's going on because the head of Alphabet is their pinchy. He's a thumbhole Brahmin from fucking India, knows exactly what's happening. So how is it on his watch? His company is throwing under the bus young, environmental and caste oppressed and religious oppressed activists like this. Where is their response to that? You know, and it's nothing. And I think that's where we have to look at, you know, black and brown bodies are excellent for markets but are really bad for human rights for these companies. So we need to really, like, hold them accountable for what's happening because, you know, we don't we don't want reparations at the end of this. We need investments that address this problem now and investments in an ambitious enough level for us to really ask for more demand for more and and really start to be architects of the future as opposed to, like repairmen for their shitty systems. Because what's working, what's happening right now is absolutely not working and

[00:36:09] Speaker2
Also building off of a lot of that anti surveillance work that you mentioned as so critical to the entire struggle. I'm very curious to also learn a little bit more about how this sort of entity has the vision for technology can align itself with and stand in solidarity with many of the other justice oriented visions of technology offered by scholars like Sophia Noble, like the Algorithmic Justice League, those projects with which to address anti blackness or other forms of systemic violence technology. How and where does antifascist technology fit in that puzzle of solidarity?

[00:36:42] Speaker3
There is a really powerful group of black scholars that are doing collaboration around these issues, and I think we need to have more engagement and a development of an entire new generation of caste thinkers who are opening the space of what this means. So I think we're going to be seeing a lot of that in the next couple of months. Like I know that we'll be writing some pieces around digital Romanism ism to try to help set a. Frame in a context around this, but it's going to be you know, this is this is the frontier we have to cross in order to really build out what we need for our people.

[00:37:23] Speaker4
I totally agree. I think, you know, like that we but it is it's an act of solidarity across all of these justice movements. And I think that in my experience at least, it's been really easy for me to explain, to explain to people what our experiences are and how this should be a protected category. It's only been challenging when I when I have to go because as people but across the countries and across companies that I've looked at, it's actually been to explain the struggle to any ordinary human being. It's it's been it's not been that hard because they can see that in action in many other walks of their life and like like them, where he said, you know, the protection is just the same protection that we offer for gender and race and all these other constructs. So I do see that this all the time because this struggle for justice, we have a common thread across other justice movements as well. And I think that, you know, when we are talking about equity and when we are talking about the I, I don't think any conversation around that would be complete without thinking about Andy Casteism and I or any company that's working in technology as well. Because India is such a big part of the technology story of any company. I don't think they can talk about equity in a holistic sense without really incorporating these discussions in and, you know, like we said, not just in terms of increasing the representation in the workforce, but also looking at it from the angle of data collection and surveillance and also borrowing decisions that they make and design decisions that they make. So, yeah, I completely agree with them.

[00:39:03] Speaker2
As we look forward also to the future, I wanted to sort of then shift gears and ask in what ways, if any, can technology be a liberating force for Dalit and other caste oppressed communities and the struggle against casteism and the fight for liberation? And more specifically, how does that inform and motivate the work that you both do as activist storytellers, technologists?

[00:39:27] Speaker3
Well, I think that technology is a tool, right? Technology is not the the platform for liberation. It's a tool towards our liberation. And I think that's significant because that level of detachment lets us make some critical decisions from when do we need tech to be free and when is tech an inhibitor to be free. And and I think that some of what we need to start being more critical about is why are we acting as these corporate surveilled platforms are Democratic engagements, particularly when we're mobilizing and doing so much social media in these surveilled places that are collaborating with people who are oppressor's. We have to think about how we can ask and demand more for what we need for our autonomy and freedom. So I think thinking about, you know, creating a next generation of Dalit entrepreneurs who can start to build a liberation tech ecosystem that looks at workers rights, that looks at, you know, a vision for what kest equity could look like and all the different ways that we're seeing those failures in big tech, I think could be very powerful. And because our community does have tech talent, our community does have people who are programmers and that are entering, you know, the workforces of these bigger entities that are just terrible. But imagine if we were able to create like an angel fund for entrepreneurs to be able to build around equitable lines. And so I think that is something I think that super important to look at. And and I also think it's important to document and document the harm and also observe and research what's happening. And so we need stakeholders in all of the pipelines that help create equitable tech, whether it's researchers, developers, you know, UX designers, content creators.

[00:41:25] Speaker3
We need to step forward into this digital realm and counter digital Brahmin ism with an age of Ambedkar where we are able to take an Ambedkar Vision into the next century. And that is a challenge Dalit and caste oppressed peoples are more than up to. And it's very critical for us to really take this direction meaningfully as far as we can, because this is how we would take Ambedkar as caravanned for Justice Forward is by lifting his analysis into these spaces that he could only have imagined. And for folks that are just hearing Ambedkar for the first time, he is a dullards civil rights leader that was the architect of the Indian constitution and trailblazer disfigures desegregation, a caste apartheid across many different Indian institutions and was a legendary thinker and polymath. And I feel like if he was alive today, he would have also found a way to become a developer just because of the kind of thinker and genius that he was. But I think that he doesn't have to be alive today because we're all children of Ambedkar who are fighters for caste abolition. And so I think we need to take that inspiration and move into these realms and understand that technology is never absence of bias, that it's actually formed a bias out of political economies that have bias and that create profit that are inherently biased. And so if we can then start to really unpack that, understand these contexts, we can build around it, we can actually create our own path to the future.

[00:43:10] Speaker4
Well, then we just gave me goosebumps, like she usually does, but every everything she said. But I also wanted to add that one little thing that has helped me and that technology has helped me with in in towards my collaboration is just helping me be connected with all of these people around the world. And like finding my wife's voice in that moment, finding people to learn from finding activist technologies, entrepreneurs, filmmakers, everybody. And, you know, in a way that I didn't feel seen before and I didn't wasn't able to find those people and find that community. I have found that right now. And I think that's something that technology as a tool has helped us with. And, you know, with everything that movie said, you know, as you know, as we get funding, as we come together around Umberto's vision, I truly see like I really have an optimistic outlook towards this. I do feel like we can build an equitable future, but it begins with envisioning that and then working backwards from it to build it with all of the resources that we have at hand.

[00:44:18] Speaker2
Absolutely, and I echo your words. The the insights you shared than where you were truly amazing and really inspiring and give us a lot of hope for the future. And as we sort of close out this incredible conversation, I wanted to just sort of ask about your both of your individual journeys through technology in your life in research and the work that you do as as you see it pertaining to these conversations. And with that, also would love to ask places for listeners to engage more with your work. Twitter handles, emails, websites, whatever you think would be best to share with our listenership today.

[00:44:59] Speaker3
I think that for folks to want to kind of track, like conversations related to cast and tech, like definitely encourage them to check out of quality labs as Instagram and Twitter and Facebook as well and put stuff there. I also really recommend that folks track what's going on with the Cisco case. And so to kind of follow up on updates related to that. Also, Alphabeat Workers Union just released a statement related to cast tech. And so they will also, from time to time, put stuff out there. So there's a lot of ways to keep connected. And I think that following our socials is like a really good way to kind of push out the resources and get connected wherever possible.

[00:45:41] Speaker4
Yeah, I second that quality labs. And then for me, I also am tracking all the things that are happening in India as well. So Internet freedom got in tracks, a lot of the surveillance issues that are happening with India and how big tech is helping the Indian fascist government. So those are two things that I look at usually

[00:46:02] Speaker2
Fantastic and will include all those links in the show notes as well. Thank you all so much for coming on the show. I think that today we really had an incredible conversation and I'm leaving this conversation feeling both troubled and inspired by all that you shared. And I'm so sure that all our listeners today feel the same way. So thank you both so much for all your work and your time today.

[00:46:28] Speaker5
We want to thank Dan Murray and Encima again for joining us today for this really wonderful conversation.

[00:46:32] Speaker1
And Nicole, a big congratulations to you for finishing out this internship.

[00:46:38] Speaker5
Thank you so much. Yes, it was really a great experience to be an intern with the podcast this semester.

[00:46:42] Speaker1
We really enjoyed having you around. And also, you originally approached Dylan and I about doing an interview on this topic a few months ago. So I'm wondering, what was it that drew you to this conversation and what is this topic mean to you?

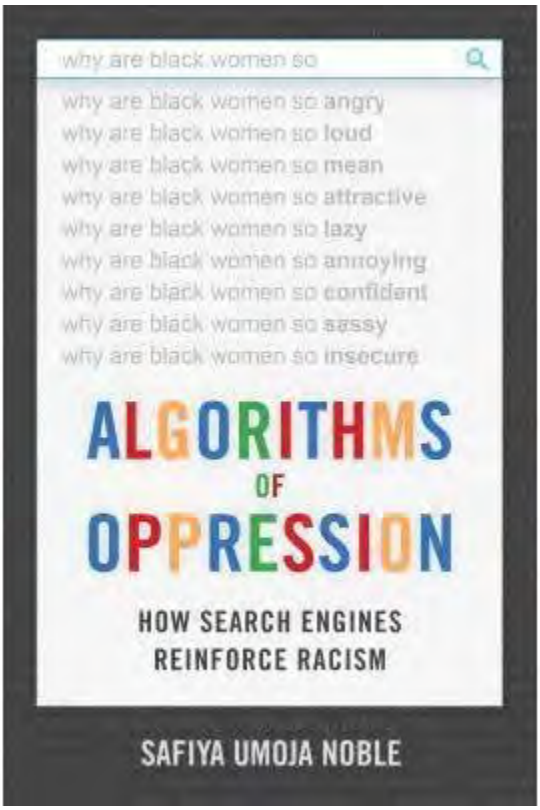
[00:46:57] Speaker5
Yeah, I think with my own background being Southasian from Brahmin Savar in our family in Silicon Valley and having benefited a lot from these structures of complicity and violence myself, I have really been interested in thinking about caste and technology from the perspective of how we can organize upper caste Indian communities and also other communities to be allies while Center and Belad feminist leadership. And so that sort of idea then to sort of make an episode about Kassin technology really appealed to me to get these conversations going and to amplify the incredible voices and insights of people like Jan and Seema. And so I was really grateful to have this conversation and to be able to platform and central to this really important discussion.

[00:47:45] Speaker1
Thank you, Nikil. And we're really grateful for you for facilitating this important conversation. And also thank you for the amazing work you've done with us over the past six months. Well, that wraps up this episode and also the radical A.I. internship. For more information on today's show, please visit the episode page at a radical. I beg. If you enjoyed this episode, we invite you to subscribe, rate and review the show on iTunes or your favorite podcast. We'll be taking a little bit of a break from our regularly scheduled episodes this summer so you can catch our new measure mentality episodes every month and you can expect our regular programming to come back around August. But until then, join our conversation on Twitter at radical iPod. And as always, stay radical.

END OF TRANSCRIPT

“A Society, Searching,” pp. 35-63

Excerpt from *Algorithms of Oppression* by Safiya Umoja Noble



just over $203 billion. At the time of the hearings, Google's latest income statement, for December 2011, showed gross profit at $24.7 billion. It had $43.3 billion cash on hand and just $6.21 billion in debt. Google held 66.2% of the search engine market industry in 2012. Google Search's profits have only continued to grow, and its holdings have become so significant that the larger company has renamed itself Alphabet, with Google Search as but one of many holdings. By the final writing of this book in August 2017, Alphabet was trading at $936.38 on NASDAQ, with a market capitalization of $649.49 billion.

The public is aware of the role of search in everyday life, and people's opinions on search are alarming. Recent data from tracking surveys and consumer-behavior trends by the comScore Media Metrix consumer panel conducted by the Pew Internet and American Life Project show that search engines are as important to Internet users as email is. Over sixty million Americans engage in search, and for the most part, people report that they are satisfied with the results they find in search engines. The 2005 and 2012 Pew reports on "search engine use" reveal that 73% of all Americans have used a search engine, and 59% report using a search engine every day.[23] In 2012, 83% of search engine users used Google. But Google Search prioritizes its own interests, and this is something far less visible to the public. Most people surveyed could not tell the difference between paid advertising and "genuine" results.

If search is so trusted, then why is a study such as this one needed? The exploration beyond that first simple search is the substance of this book. Throughout the discussion of these and other results, I want to emphasize the main point: there is a missing social context in commercial digital media platforms, and it matters, particularly for marginalized groups that are problematically represented in stereotypical or pornographic ways, for those who are bullied, and for those who are consistently targeted. I use only a handful of illustrative searches to underscore the point and to raise awareness—and hopefully intervention—of how important what we find on the web through commercial search engines is to society.

Search Results as Power

Search results reflect the values and norms of the search company's commercial partners and advertisers and often reflect our lowest and

most demeaning beliefs, because these ideas circulate so freely and so often that they are normalized and extremely profitable. Search results are more than simply what is popular. The dominant notion of search results as being both "objective" and "popular" makes it seem as if misogynist or racist search results are a simple mirror of the collective. Not only do problematic search results seem "normal," but they seem completely unavoidable as well, even though these ideas have been thoroughly debunked by scholars. Unfortunately, users of Google give consent to the algorithms' results through their continued use of the product, which is largely unavoidable as schools, universities, and libraries integrate Google products into our educational experiences.[24]

Google's monopoly status,[25] coupled with its algorithmic practices of biasing information toward the interests of the neoliberal capital and social elites in the United States, has resulted in a provision of information that purports to be credible but is actually a reflection of advertising interests. Stated another way, it can be argued that Google functions in the interests of its most influential paid advertisers or through an intersection of popular and commercial interests. Yet Google's users think of it as a public resource, generally free from commercial interest. Further complicating the ability to contextualize Google's results is the power of its social hegemony.[26] Google benefits directly and materially from what can be called the "labortainment"[27] of users, when users consent to freely give away their labor and personal data for the use of Google and its products, resulting in incredible profit for the company.

There are many cases that could be made to show how overreliance on commercial search by the public, including librarians, information professionals, and knowledge managers—all of whom are susceptible to overuse of or even replacement by search engines—is something that we must pay closer attention to right now. Under the current algorithmic constraints or limitations, commercial search does not provide appropriate social, historical, and contextual meaning to already overracialized and hypersexualized people who materially suffer along multiple axes. In the research presented in this study, the reader will find a more meaningful understanding of the kind of harm that such limitations can cause for users reliant on the web as an artifact of both formal and informal culture.[28] In sum, search results play a powerful role in providing fact and authority to those who see them, and as such, they must

be examined carefully. Google has become a central object of study for digital media scholars,[29] due to recognition on these scholars' parts of the power and impact wielded by the necessity to begin most engagements with social media via a search process and the near universality with which Google has been adopted and embedded into all aspects of the digital media landscape to respond to that need. This work is addressing a gap in scholarship on how search works and what it biases, public trust in search, the relationship of search to information studies, and the ways in which African Americans, among others, are mediated and commodified in Google.

To start revealing some of the processes involved, it is important to think about how results appear. Although one might believe that a query to a search engine will produce the most relevant and therefore useful information, it is actually predicated on a matrix of ways in which pages are hyperlinked and indexed on the web.[30] Rendering web content (pages) findable via search engines is an expressly social, economic, and human project, which several scholars have detailed. These renderings are delivered to users through a set of steps (algorithms) implemented by programming code and then naturalized as "objective." One of the reasons this is seen as a neutral process is because algorithmic, scientific, and mathematical solutions are evaluated through procedural and mechanistic practices, which in this case includes tracing hyperlinks among pages. This process is defined by Google's founders, Sergey Brin and Larry Page, as "voting," which is the term they use to describe how search results move up or down in a ranked list of websites. For the most part, many of these processes have been automated, or they happen through graphical user interfaces (GUIs) that allow people who are not programmers (i.e., not working at the level of code) to engage in sharing links to and from websites.[31]

Research shows that users typically use very few search terms when seeking information in a search engine and rarely use advanced search queries, as most queries are different from traditional offline information-seeking behavior.[32] This front-end behavior of users appears to be simplistic; however, the information retrieval systems are complex, and the formulation of users' queries involves cognitive and emotional processes that are not necessarily reflected in the system design.[33] In essence, while users use the simplest queries they can in a

search box because of the way interfaces are designed, this does not always reflect how search terms are mapped against more complex thought patterns and concepts that users have about a topic. This disjunction between, on the one hand, users' queries and their real questions and, on the other, information retrieval systems makes understanding the complex linkages between the content of the results that appear in a search and their import as expressions of power and social relations of critical importance.

The public generally trusts information found in search engines. Yet much of the content surfaced in a web search in a commercial search engine is linked to paid advertising, which in part helps drive it to the top of the page rank, and searchers are not typically clear about the distinctions between "real" information and advertising. Given that advertising is a fundamental part of commercial search, using content analysis to make sense of what *actually* is served up in search is appropriate and consistent with the articulation of feminist critiques of the images of women in print advertising.[34] These scholars have shown the problematic ways that women have been represented—as sex objects, incompetent, dependent on men, or underrepresented in the workforce[35]—and the content and representation of women and girls in search engines is consistent with the kinds of problematic and biased ideas that live in other advertising channels. Of course, this makes sense, because Google Search is in fact an advertising platform, not intended to solely serve as a public information resource in the way that, say, a library might. Google creates advertising algorithms, not information algorithms.

To understand search in the context of this book, it is important to look at the description of the development of Google outlined by the former Stanford computer science graduate students and cofounders of the company, Sergey Brin and Larry Page, in "The Anatomy of a Large-Scale Hypertextual Web Search Engine." Their paper, written in graduate school, serves as the architectural framework for Google's PageRank. In addition, it is crucial to also look at the way that citation analysis, the foundational notion behind Brin and Page's idea, works as a bibliometric project that has been extensively developed by library and information science scholars. Both of these dynamics are often misunderstood because they do not account for the complexities of human intervention involved in vetting of information, nor do they pay attention

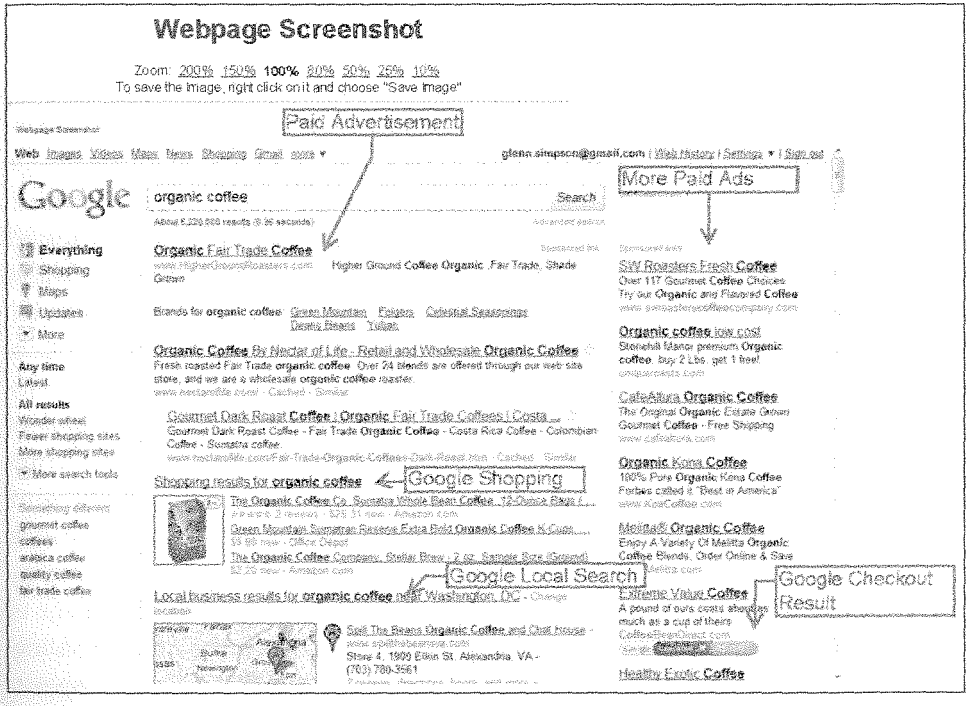


Figure 1.11. Example of Google's prioritization of its own properties in web search. Source: Inside Google (2010).

to the relative weight or importance of certain types of information.[36] For example, in the process of citing work in a publication, all citations are given equal weight in the bibliography, although their relative importance to the development of thought may not be equal at all. Additionally, no relative weight is given to whether a reference is validated, rejected, employed, or engaged—complicating the ability to know what a citation actually *means* in a document. Authors who have become so mainstream as not to be cited, such as not attributing modern discussions of class or power dynamics to Karl Marx or the notion of "the individual" to the scholar of the Italian Renaissance Jacob Burckhardt, mean that these intellectual contributions may undergird the framework of an argument but move through works without being cited any longer. Concepts that may be widely understood and accepted ways of knowing are rarely cited in mainstream scholarship, an important dynamic that

Linda Smith, former president of the Association for Information Science and Technology (ASIS&T) and associate dean of the Information School at the University of Illinois at Urbana-Champaign, argues is part of the flawed system of citation analysis that deserves greater attention if bibliometrics are to serve as a legitimating force for valuing knowledge production.

Brin and Page saw the value in using works that others cite as a model for thinking about determining what is legitimate on the web, or at least to indicate what is popular based on many people acknowledging particular types of content. In terms of outright co-optation of the citation, vis-à-vis the hyperlink, Brin and Page were aware of some of the challenges I have described. They were clearly aware from the beginning of the potential for "gaming" the system by advertising companies or commercial interests, a legitimated process now known as "search engine optimization," to drive ads or sites to the top of a results list for a query, since clicks on web links can be profitable, as are purchases gained by being vetted as "the best" by virtue of placement on the first page of PageRank. This is a process used for web results, not paid advertising, which is often highlighted in yellow (see figure 1.6). Results that appear not to be advertising are in fact influenced by the advertising algorithm. In contrast to scientific or scholarly citations, which once in print are persistent and static, hyperlinking is a dynamic process that can change from moment to moment.[37] As a result, the stability of results in Google ranking shifts and is prone to being affected by a number of processes that I will cover, primarily search engine optimization and advertising. This means that results shift over time. The results of what is most hyperlinked using Google's algorithm today will be different at a later date or from the time that Google's web-indexing crawlers move through the web until the next cycle.[38]

Citation importance is a foundational concept for determining scholarly relevance in certain disciplines, and citation analysis has largely been considered a mechanism for determining whether a given article or scholarly work is important to the scholarly community. I want to revisit this concept because it also has implications for thinking about the legitimation of information, not just citability or popularity. It is also a function of human beings who are engaged in a curation practice, not entirely left to automation. Simply put, if scholars choose to

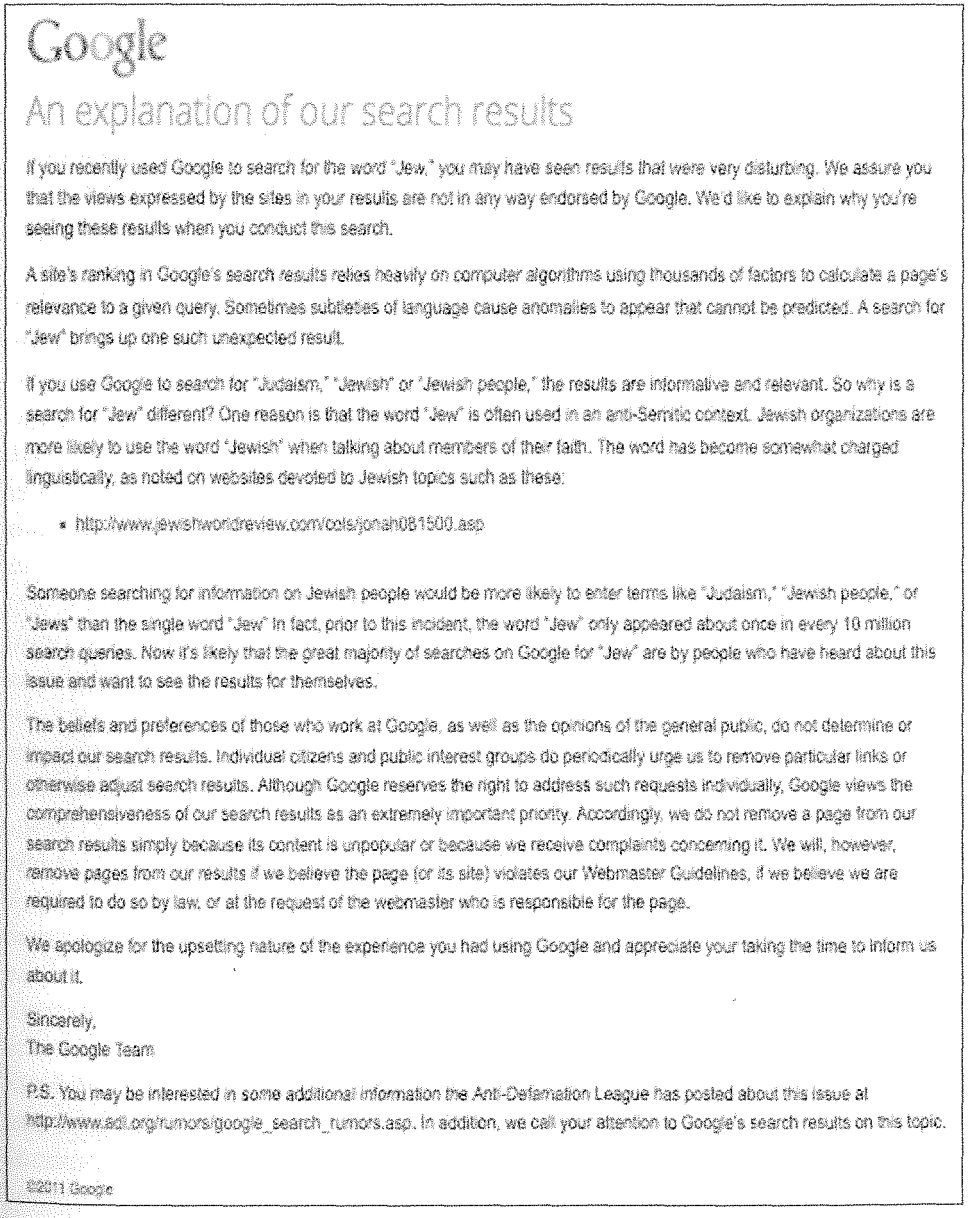
cite a study or document, they have signaled its relevance; thus, human beings (scholars) are involved in making decisions about a document's relevance, although all citations in a bibliography do not share the same level of meaningfulness. Building on this concept of credibility through citation, PageRank is what Brin and Page call the greater likelihood that a document is relevant "if there are many pages that point to it" versus "the probability that the random surfer visits a page."[39] In their research, which led to the development of Google Search, Brin and Page discuss the possibility of monopolizing and manipulating keywords through commercialization of the web search process. Their information-retrieval goal was to deliver the most relevant or very best ten or so documents out of the possible number of documents that could be returned from the web. The resulting development of their search architecture is PageRank—a system that is based on "the objective measure of its citation importance that corresponds well with people's subjective idea of importance."[40]

One of the most profound parts of Brin and Page's work is in appendix A, in which they acknowledge the ways that commercial interests can compromise the quality of search result retrieval. They state, citing Ben Bagdikian, "It is clear that a search engine which was taking money for showing cellular phone ads would have difficulty justifying the page that our system returned to its paying advertisers. For this type of reason and historical experience with other media, we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."[41] Brin and Page outline a clear roadmap for how bias would work in advertising-oriented search and the effects this would have, and they directly suggest that it is in the consumer's interest not to have search compromised by advertising and commercialism. To some degree, PageRank was intended to be a measure of relevance based on popularity—including what both web surfers and web designers link to from their sites. As with academic citations, Brin and Page decided that citation analysis could be used as a model for determining whether web links could be ranked according to their importance by measuring how much they were back-linked or hyperlinked to or from. Thus, the model for web indexing pages was born. However, in the case of citation analysis, a scholarly author goes through several stages of vetting and credibility testing, such as the peer-review process,

before work can be published and cited. In the case of the web, such credibility checking is not a factor in determining what will be hyperlinked. This was made explicitly clear in the many news reports covering the 2016 U.S. presidential election, where clickbait and manufactured "news" from all over the world clouded accurate reporting of facts on the presidential candidates.

Another example of the shortcomings of removing this human curation or decision making from the first page of results at the top of PageRank, in addition to the results that I found for "black girls," can be found in the more public dispute over the results that were returned on searches for the word "Jew," which included a significant number of anti-Semitic pages. As can be seen by Google's response to the results of a keyword search for "Jew," Google takes little responsibility toward the ways that it provides information on racial and gendered identities, which are curated in more meaningful ways in scholarly databases. Siva Vaidhyanathan's 2011 book *The Googlization of Everything (And Why We Should Worry)* chronicles recent attempts by the Jewish community and Anti-Defamation League to challenge Google's priority ranking to the first page of anti-Semitic, Holocaust-denial websites. So troublesome were these search results that in 2011, Google issued a statement about its search process, encouraging people to use "Jews" and "Jewish people" in their searches, rather than the seemingly pejorative term "Jew"—claiming that the company can do nothing about the word's co-optation by White supremacist groups (see figure 1.12).

Google, according to its own disclaimer, will only remove pages that are considered unlawful, as is the case in France and Germany, where selling or distributing neo-Nazi materials is prohibited. Without such limits on derogatory, racist, sexist, or homophobic materials, Google allows its algorithm—which is, as we can see, laden with what Diaz calls "sociopolitics"—to stand without debate while protesting its inability to remove pages. As recently as June 27, 2012, Google settled a claim by the French antiracism organization the International League Against Racism over Google's use of ethnic identity—"Jew"—in association with popular searches.[42] Under French law, racial identity markers cannot be stored in databases, and the auto-complete techniques used in the Google search box link names of people to the word "Jew" on the basis of past user searches. What this recent case points to is another effort to



Google

An explanation of our search results

If you recently used Google to search for the word "Jew," you may have seen results that were very disturbing. We assure you that the views expressed by the sites in your results are not in any way endorsed by Google. We'd like to explain why you're seeing these results when you conduct this search.

A site's ranking in Google's search results relies heavily on computer algorithms using thousands of factors to calculate a page's relevance to a given query. Sometimes subtleties of language cause anomalies to appear that cannot be predicted. A search for "Jew" brings up one such unexpected result.

If you use Google to search for "Judaism," "Jewish" or "Jewish people," the results are informative and relevant. So why is a search for "Jew" different? One reason is that the word "Jew" is often used in an anti-Semitic context. Jewish organizations are more likely to use the word "Jewish" when talking about members of their faith. The word has become somewhat charged linguistically, as noted on websites devoted to Jewish topics such as these:

- http://www.jewishworldreview.com/cols/jonah081500.asp

Someone searching for information on Jewish people would be more likely to enter terms like "Judaism," "Jewish people," or "Jews" than the single word "Jew." In fact, prior to this incident, the word "Jew" only appeared about once in every 10 million search queries. Now it's likely that the great majority of searches on Google for "Jew" are by people who have heard about this issue and want to see the results for themselves.

The beliefs and preferences of those who work at Google, as well as the opinions of the general public, do not determine or impact our search results. Individual citizens and public interest groups do periodically urge us to remove particular links or otherwise adjust search results. Although Google reserves the right to address such requests individually, Google views the comprehensiveness of our search results as an extremely important priority. Accordingly, we do not remove a page from our search results simply because its content is unpopular or because we receive complaints concerning it. We will, however, remove pages from our results if we believe the page (or its site) violates our Webmaster Guidelines, if we believe we are required to do so by law, or at the request of the webmaster who is responsible for the page.

We apologize for the upsetting nature of the experience you had using Google and appreciate your taking the time to inform us about it.

Sincerely,
The Google Team

P.S. You may be interested in some additional information the Anti-Defamation League has posted about this issue at http://www.adl.org/rumors/google_search_rumors.asp. In addition, we call your attention to Google's search results on this topic.

Figure 1.12. Explanation of results by Google. Source: www.google.com/explanation.html (originally available in 2005).

redefine distorted images of people in new media. These cases of distortion, however, continue to accumulate.

The public's as well as the Jewish community's interest in accurate information about Jewish culture and the Holocaust should be enough motivation to provoke a national discussion about consumer harm, to which my research shows we can add other cultural and gender-based identities that are misrepresented in search engines. However, Google's assertion that its search results, though problematic, were computer generated (and thus not the company's fault) was apparently a good-enough answer for the Anti-Defamation League (ADL), which declared, "We are extremely pleased that Google has heard our concerns and those of its users about the offensive nature of some search results and the unusually high ranking of peddlers of bigotry and anti-Semitism."[43] The ADL does acknowledge on its website its gratitude to Sergey Brin, cofounder of Google and son of Russian Jewish immigrants, for his personal letter to the organization and his mea culpa for the "Jew" search-term debacle. The ADL generously stated in its press release about the incident that Google, as a resource to the public, should be forgiven because "until the technical modifications are implemented, Google has placed text on its site that gives users a clear explanation of how search results are obtained. Google searches are automatically determined using computer algorithms that take into account thousands of factors to calculate a page's relevance."[44]

If there is a technical fix, then what are the constraints that Google is facing such that eight years later, the issue has yet to be resolved? A search for the word "Jew" in 2012 produces a beige box at the bottom of the results page from Google linking to its lengthy disclaimer about the results—which remain a mix of both anti-Semitic and informative sites (see figure 1.13). That Google places the responsibility for bad results back on the shoulders of information searchers is a problem, since most of the results that the public gets on broad or open-ended racial and gendered searches are out of their control and entirely within the control of Google Search.

It is important to note that Google has conceded the fact that anti-Semitism as the primary information result about Jewish people is a problem, despite its disclaimer that tries to put the onus for bad results on the searcher. In Germany and France, for example, it is illegal to sell

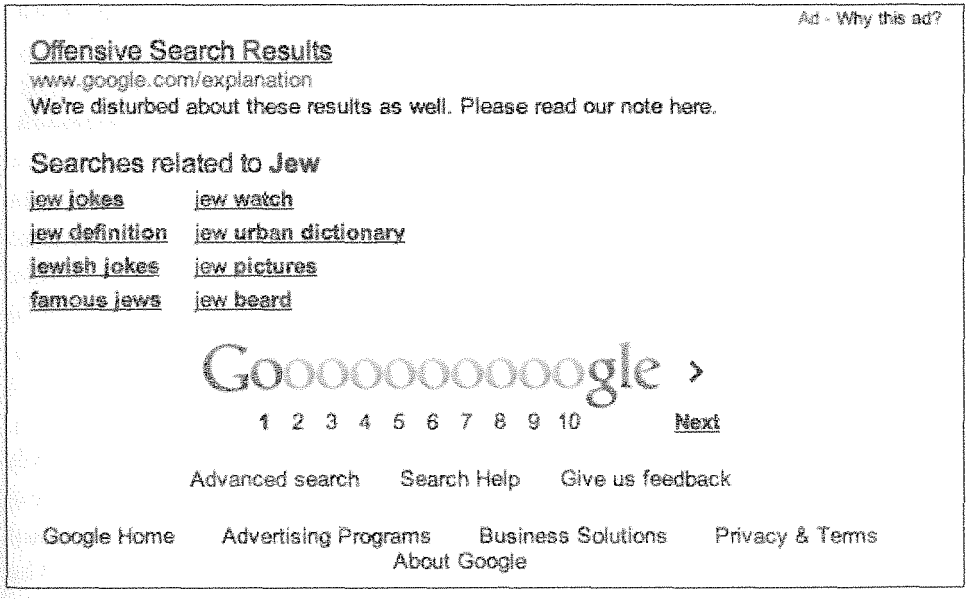


Figure 1.13. Google's bottom-of-the-page beige box regarding offensive results, which previously took users to "An Explanation of Our Search Results." Source: www.google.com/explanation (no longer available).

Nazi memorabilia, and Google has had to put in place filters that ensure online retailers of such are not visible in search results. In 2002, Benjamin Edelman and Jonathan Zittrain at Harvard University's Berkman Center for Internet and Society concluded that Google was filtering its search results in accordance with local law and precluding neo-Nazi organizations and content from being displayed.[45] While this indicates that Google can in fact remove objectionable hits, it is equally troubling, because the company provided search results without informing searchers that information was being deleted. That is to say that the results were presented as factual and complete without mention of omission. Yahoo!, another leading U.S. search engine, was forced into a protracted legal battle in France for allowing pro-Nazi memorabilia to be sold through its search engine, in violation of French law. What these cases point to is that search results are deeply contextual and easily manipulated, rather than objective, consistent, and transparent, and that they can be legitimated only in social, political, and historical context.

The issue of unlawfulness over the harm caused by derogatory results is a question of considerable debate. For example, in the United States, where free speech protections are afforded to all kinds of speech, including hate speech and racist or sexist depictions of people and communities, there is a higher standard of proof required to show harm toward disenfranchised or oppressed people. We need legal protections now more than ever, as automated decision-making systems wield greater power in society.

Gaming the System: Optimizing and Co-opting Results in Search Engines

Google's advertising tool or optimization product is AdWords. AdWords allows anyone to advertise on Google's search pages and is highly customizable. With this tool, an advertiser can set a maximum amount of money that it wants to spend on a daily basis for advertising. The model for AdWords is that Google will display ads on search pages that it believes are relevant to the kind of search query that is taking place by a user. If a user clicks on an ad, then the advertiser pays. And Google incentivizes advertisers by suggesting that their ads will show up in searches and display, but the advertiser (or Google customer) pays for the ad only when a user (Google consumer) clicks on the advertisement, which is the cost per click (CPC). The advertiser selects a series of "keywords" that it believes closely align with its product or service that it is advertising, and a customer can use a Keyword Estimator tool in order to see how much the keywords they choose to associate with their site might cost. This advertising mechanism is an essential part of how PageRank prioritizes ads on a page, and the association of certain keywords with particular industries, products, and services derives from this process, which works in tandem with PageRank.

In order to make sense of the specific results in keyword searches, it is important to know how Google's PageRank works, what commercial processes are involved in PageRank, how search engine optimization (SEO) companies have been developed to influence the process of moving up results,[46] and how Google bombing[47] occurs on occasion. Google bombing is the practice of excessively hyperlinking to a website (repeatedly coding HTML to link a page to a term or phrase) to cause it to

rise to the top of PageRank, but it is also seen as a type of "hit and run" activity that can deliberately co-opt terms and identities on the web for political, ideological, and satirical purposes. Judit Bar-Ilan, a professor of information science at Bar-Ilan University, has studied this practice to see if the effect of forcing results to the top of PageRank has a lasting effect on the result's persistence, which can happen in well-orchestrated campaigns. In essence, Google bombing is the process of co-opting content or a term and redirecting it to unrelated content. Internet lore attributes the creation of the term "Google bombing" to Adam Mathes, who associated the term "talentless hack" with a friend's website in 2001. Practices such as Google bombing (also known as Google washing) are impacting both SEO companies and Google alike. While Google is invested in maintaining the quality of search results in PageRank and policing companies that attempt to "game the system," as Brin and Page foreshadowed, SEO companies do not want to lose ground in pushing their clients or their brands up in PageRank.[48] SEO is the process of "using a range of techniques, including augmenting HTML code, web page copy editing, site navigation, linking campaigns and more, in order to improve how well a site or page gets listed in search engines for particular search topics,"[49] in contrast to "paid search," in which the company pays Google for its ads to be displayed when specific terms are searched. A media spectacle of this nature is the case of Senator Rick Santorum, Republican of Pennsylvania, whose website and name were associated with insults in order to drive objectionable content to the top of PageRank.[50] Others who have experienced this kind of co-optation of identity or less-than-desirable association of their name with an insult include former president George W. Bush and the pop singer Justin Bieber.

All of these practices of search engine optimization and Google bombing can take place independently of and in concert with the process of crawling and indexing the web. In fact, being found gives meaning to a website and creates the conditions in which a ranking can happen. Search engine optimization is a major factor in findability on the web. What is important to note is that search engine optimization is a multibillion-dollar industry that impacts the value of specific keywords; that is, marketers are invested in using particular keywords, and keyword combinations, to optimize their rankings.

Figure 1.14. Example of a Google bomb on George W. Bush and the search terms "miserable failure," 2005.

Despite the widespread beliefs in the Internet as a democratic space where people have the power to dynamically participate as equals, the Internet is in fact organized to the benefit of powerful elites,[51] including corporations that can afford to purchase and redirect searches to their own sites. What is most popular on the Internet is not wholly a matter of what users click on and how websites are hyperlinked—there are a variety of processes at play. Max Holloway of *Search Engine Watch* notes, "Similarly, with Google, when you click on a result—or, for that matter, don't click on a result—that behavior impacts future results. One consequence of this complexity is difficulty in explaining system behavior. We primarily rely on performance metrics to quantify the success or failure of retrieval results, or to tell us which variations of a system work better than others. Such metrics allow the system to be continuously improved upon."[52] The goal of combining search terms, then, in the context of the landscape of the search engine optimization logic, is only the beginning.

Much research has now been done to dispel the notion that users of the Internet have the ability to "vote" with their clicks and express interest in individual content and information, resulting in democratic practices online.[53] Research shows the ways that political news and information in the blogosphere are mediated and directed such that major news outlets surface to the top of the information pile over less well-known websites and alternative news sites in the blogosphere, to the benefit of elites.[54] In the case of political information seeking, research has shown how Google directs web traffic to mainstream corporate news conglomerates, which increases their ability to shape the political discourse. Google too is a mediating platform that, at least at one moment in time, in September 2011, allowed the porn industry to take precedence in the representations of Black women and girls over other possibilities among at least eleven and a half billion documents that could have been indexed.[55] That moment in 2011 is, however, emblematic of Google's ongoing dynamic. It has since produced many more problematic results.

As the Federal Communications Commission declares broadband "the new common medium,"[56] the role of search engines is taking on even greater importance to "the widest possible dissemination of information from diverse and antagonistic sources . . . essential to the welfare of the public."[57] This political economy of search engines and traditional advertisers includes search engine optimization companies that operate in a secondary or gray market (often in opposition to Google). Ultimately, the results we get are about the financial interest that Google or SEOs have in helping their own clients optimize their rankings. In fact, Google is in the business of selling optimization. Extensive critiques of Google have been written on the political economy of search[58] and the way that consolidations in the search engine industry market contribute to the erosion of public resources, in much the way that the media scholars Robert McChesney, former host of nationally syndicated radio show *Media Matters*, and John Nichols, a writer for the *Nation*, critique the consolidation of the mass-media news markets. Others have spoken to the inherent democratizing effect of search engines, such that search is adding to the diversity of political organization and discourse because the public is able to access more information in the marketplace of ideas.[59] Mounting evidence shows that automated decision-making systems are disproportionately harmful to the most vulnerable and the

least powerful, who have little ability to intervene in them—from misrepresentation to prison sentencing to accessing credit and other life-impacting formulas.

This landscape of search engines is important to consider in understanding the meaning of search for the public, and it serves as a basis for examining why information quality online is significant. We must trouble the notion of Google as a public resource, particularly as institutions become more reliant on Google when looking for high-quality, contextualized, and credible information. This shift from public institutions such as libraries and schools as brokers of information to the private sector, in projects such as Google Books, for example, is placing previously public assets in the hands of a multinational corporation for private exploitation. Information is a new commodity, and search engines can function as private information enclosures.[60] We need to make more visible the commercial interests that overdetermine what we can find online.

The Enclosure of the Public Domain through Search Engines

At the same time that search engines have become the dominant portal for information seeking by U.S. Internet users, the rise of commercial mediation of information in those same search engines is further enclosing the public domain. Decreases in funding for public information institutions such as libraries and educational institutions and shifts of responsibility to individuals and the private sector have reframed the ways that the public conceives of what can and should be in the public domain. Yet Google Search is conceived of as a public resource, even though it is a multinational advertising company. These shifts of resources that were once considered public have been impacted by increased intellectual property rights, licensing, and publishing agreements for companies and private individuals in the domain of copyrights, patents, and other legal protections. The move of community-based assets and culture to private hands is arguably a crisis that has rolled back the common good, but there are still possible strategies that can be explored for maintaining what can remain in the public domain. Commercial control over the Internet, often considered a "commons," has moved it further away from the public through a series of national and international regulations and intellectual and commercial borders that exist in the management of the

network.[61] Beyond the Internet and the control of the network, public information—whether delivered over the web or not—continues to be outsourced to the private sphere, eroding the public information commons that has been a basic tenet of U.S. democracy.

The critical media scholar Herbert Schiller, whose work foreshadowed many of the current challenges in the information and communications landscape, provides a detailed examination of the impact of outsourcing and deregulation in the spheres of communication and public information. His words are still timely: "The practice of selling government (or any) information serves the corporate user well. Ordinarily individual users go to the end of the dissemination queue. Profoundly antidemocratic in its effect, privatizing and/or selling information, which at one time was considered public property, has become a standard practice in recent years."[62] What this critique shows is that the privatization and commercial nature of information has become so normalized that it not only becomes obscured from view but, as a result, is increasingly difficult to critique within the public domain. The Pew Internet and American Life Project corroborates that the public trusts multinational corporations that provide information over the Internet and that there is a low degree of distrust of the privatization of information.[63] Part of this process of acquiescence to the increased corporatization of public life can be explained by the economic landscape, which is shaped by military-industrial projects such as the Internet that have emerged in the United States,[64] increasing the challenge of scholars who are researching the impact of such shifts in resources and accountability. Molly Niesen at the University of Illinois has written extensively on the loss of public accountability by federal agencies such as the Federal Trade Commission (FTC), which is a major contribution to our understanding of where the public can focus attention on policy interventions.[65] We should leverage her research to think about the FTC as the key agency to manage and intervene in how corporations control the information landscape.

The Cultural Power of Algorithms

The public is minimally aware of these shifts in the cultural power and import of algorithms. In a 2015 study by the Pew Research Center,

Figure 1.15. *Forbes*'s online reporting (and critique) of the Epstein and Robertson study.

"American's Privacy Strategies Post-Snowden," only 34% of respondents who were aware of the surveillance that happens automatically online through media platforms, such as search behavior, email use, and social media, reported that they were shifting their online behavior because of concerns of government surveillance and the potential implications or harm that could come to them.[66] Little of the American public knows that online behavior has more importance than ever. Indeed, Internet-based activities are dramatically affecting our notions of how democracy and freedom work, particularly in the realm of the free flow of information and communication. Our ability to engage with the information landscape subtly and pervasively impacts our understanding of the world and each other.

An example of how information flow and bias in the realm of politics have recently come to the fore can be found in an important new study about how information bias can radically alter election outcomes. The former editor of *Psychology Today* and professor Robert Epstein and Ronald Robertson, the associate director of the American Institute for Behavioral Research and Technology, found in their 2013 study that democracy was at risk because manipulating search rankings could shift voters' preferences, substantially and without their awareness. In their study, they note that the tenor of stories about a candidate in search engine results, whether favorable or unfavorable, dramatically af-

fected the way that people voted. Seventy-five percent of participants were not aware that the search results had been manipulated. The researchers concluded, "The outcomes of real elections—especially tight races—can conceivably be determined by the strategic manipulation of search engine rankings and . . . that the manipulation can be accomplished without people being aware of it. We speculate that unregulated search engines could pose a serious threat to the democratic system of government."[67]

In March 2012, the Pew Internet and American Life Project issued an update to its 2005 "Search Engine Users" study. The 2005 and 2012 surveys tracking consumer-behavior trends from the comScore Media Metrix consumer panel show that search engines are as important to Internet users as email is. In fact, the *Search Engine Use 2012* report suggests that the public is "more satisfied than ever with the quality of search results."[68] Further findings include the following:

- 73% of all Americans have used a search engine, and 59% report using a search engine every day.
- 83% of search engine users use Google.

Especially alarming is the way that search engines are increasingly positioned as a trusted public resource returning reliable and credible information. According to Pew, users report generally good outcomes and relatively high confidence in the capabilities of search engines:

- 73% of search engine users say that most or all the information they find as they use search engines is accurate and trustworthy.

Yet, at the same time that search engine users report high degrees of confidence in their skills and trust in the information they retrieve from engines, they have also reported that they are naïve about how search engines work:

- 62% of search engine users are not aware of the difference between paid and unpaid results; that is, only 38% are aware, and only 8% of search engine users say that they can always tell which results are paid or sponsored and which are not.

- In 2005, 70% of search engine users were fine with the concept of paid or sponsored results, but in 2012, users reported that they are not okay with targeted advertising because they do not like having their online behavior tracked and analyzed.
- In 2005, 45% of search engine users said they would stop using search engines if they thought the engines were not being clear about offering some results for pay.
- In 2005, 64% of those who used engines at least daily said search engines are a fair and unbiased source of information; the percentage increased to 66% in 2012.

Users in the 2012 Pew study also expressed concern about personalization:

- 73% reported that they would *not be okay* with a search engine keeping track of searches and using that information to personalize future search results. Participants reported that they feel this to be an invasion of privacy.

In the context of these concerns, a 2011 study by the researchers Martin Feuz and Matthew Fuller from the Centre for Cultural Studies at the University of London and Felix Stalder from the Zurich University of the Arts found that personalization is not simply a service to users but rather a mechanism for better matching consumers with advertisers and that Google's personalization or aggregation is about actively matching people to groups, that is, categorizing individuals.[69] In many cases, different users are seeing similar content to each other, but users have little ability to see how the platform is attempting to use prior search history and demographic information to shape their results. Personalization is, to some degree, giving people the results they want on the basis of what Google knows about its users, but it is also generating results for viewers to see what Google Search thinks might be good for advertisers by means of compromises to the basic algorithm. This new wave of interactivity, without a doubt, is on the minds of both users and search engine optimizing companies and agencies. Google applications such as Gmail or Google Docs and social media sites such as Facebook track identity and previous searches in order to surface targeted ads for users by analyzing users' web traces. So not only do search engines increasingly remember the digital traces of where we have been

and what links we have clicked in order to provide more custom content (a practice that has begun to gather more public attention after Google announced it would use past search practices and link them to users in its privacy policy change in 2012),[70] but search results will also vary depending on whether filters to screen out porn are enabled on computers.[71]

It is certain that information that surfaces to the top of the search pile is not exactly the same for every user in every location, and a variety of commercial advertising, political, social, and economic decisions are linked to the way search results are coded and displayed. At the same time, results are generally quite similar, and complete search personalization—customized to very specific identities, wants, and desires—has yet to be developed. For now, this level of personal-identity personalization has less impact on the variation in results than is generally believed by the public.

Losing Control of Our Images and Ourselves in Search

It is well known that traditional media have been rife with negative or stereotypical images of African American / Black people,[72] and the web as the locus of new media is a place where traditional media interests are replicated. Those who have been inappropriately and unfairly represented in racist and sexist ways in old media have been able to cogently critique those representations and demand expanded representations, protest stereotypes, and call for greater participation in the production of alternative, nonstereotypical or oppressive representations. This is part of the social charge of civil rights organizations such as the Urban League[73] and the National Association for the Advancement of Colored People, which monitor and report on minority misrepresentations, as well as celebrate positive portrayals of African Americans in the media.[74] At a policy level, some civil rights organizations and researchers such as Darnell Hunt, dean of the division of social science and department chair of sociology at UCLA,[75] have been concerned with media representations of African Americans, and mainstream organizations such as Free Press have been active in providing resources about the impact of the lack of diversity, stereotyping, and hate speech in the media. Indeed, some of these resources have been directed toward net-neutrality issues

and closing the digital divide.[76] Media advocacy groups that focus on the pornification of women or the stereotyping of people of color might turn their attention toward the Internet as another consolidated media resource, particularly given the evidence showing Google's information and advertising monopoly status on the web.

Bias in Search

"Traffic Report: How Google Is Squeezing Out Competitors and Muscling Into New Markets," by ConsumerWatchdog.org's Inside Google (June 2010), details how Google effectively blocks sites that it competes with and prioritizes its own properties to the top of the search pile (YouTube over other video sites, Google Maps over MapQuest, and Google Images over Photobucket and Flickr). The report highlights the process by which Universal Search is not a neutral and therefore universal process but rather a commercial one that moves sites that buy paid advertising to the top of the pile. Amid these practices, the media, buttressed by an FTC investigation,[77] have suggested that algorithms are not at all unethical or harmful because they are free services and Google has the right to run its business in any way it sees fit. Arguably, this is true, so true that the public should be thoroughly informed about the ways that Google biases information—toward largely stereotypic and decontextualized results, at least when it comes to certain groups of people. Commercial platforms such as Facebook and YouTube go to great lengths to monitor uploaded user content by hiring web content screeners, who at their own peril screen illicit content that can potentially harm the public.[78] The expectation of such filtering suggests that such sites vet content on the Internet on the basis of some objective criteria that indicate that some content is in fact quite harmful to the public. New research conducted by Sarah T. Roberts in the Department of Information Studies at UCLA shows the ways that, in fact, commercial content moderation (CCM, a term she coined) is a very active part of determining what is allowed to surface on Google, Yahoo!, and other commercial text, video, image, and audio engines.[79] Her work on video content moderation elucidates the ways that commercial digital media platforms currently outsource or in-source image and video content filtering to comply with their terms of use

agreements. What is alarming about Roberts's work is that it reveals the processes by which content is already being screened and assessed according to a continuum of values that largely reflect U.S.-based social norms, and these norms reflect a number of racist and stereotypical ideas that make screening racism and sexism and the abuse of humans in racialized ways "in" and perfectly acceptable, while other ideas such as the abuse of animals (which is also unacceptable) are "out" and screened or blocked from view. She details an interview with one of the commercial content moderators (CCMs) this way:

> We have very, very specific itemized internal policies . . . the internal policies are not made public because then it becomes very easy to skirt them to essentially the point of breaking them. So yeah, we had very specific internal policies that we were constantly, we would meet once a week with SecPol to discuss, there was one, blackface is not technically considered hate speech by default. Which always rubbed me the wrong way, so I had probably ten meltdowns about that. When we were having these meetings discussing policy and to be fair to them, they always listened to me, they never shut me up. They didn't agree, and they never changed the policy but they always let me have my say, which was surprising. (Max Breen, MegaTech CCM Worker).

The MegaTech example is an illustration of the fact that social media companies and platforms make active decisions about what kinds of racist, sexist, and hateful imagery and content they will host and to what extent they will host it. These decisions may revolve around issues of "free speech" and "free expression" for the user base, but on commercial social media sites and platforms, these principles are always counterbalanced by a profit motive; if a platform were to become notorious for being too restrictive in the eyes of the majority of its users, it would run the risk of losing participants to offer to its advertisers. So MegaTech erred on the side of allowing more, rather than less, racist content, in spite of the fact that one of its own CCM team members argued vociferously against it and, by his own description, experienced emotional distress ("meltdowns") around it.[80]

This research by Roberts, particularly in the wake of leaked reports from Facebook workers who perform content moderation, suggests that people and policies are put in place to navigate and moderate content on the web. Egregious and racist content, content that is highly profitable, proliferates because many tech platforms are interested in attracting the interests and attention of the majority in the United States, not of racialized minorities.

Challenging Race- and Gender-Neutral Narratives

These explorations of web results on the first page of a Google search also reveal the default identities that are protected on the Internet or are less susceptible to marginalization, pornification, and commodification. The research of Don Heider, the dean of Loyola University Chicago's School of Communication, and Dustin Harp, an assistant professor in the Department of Communication at the University of Texas, Arlington, shows that even though women constitute just slightly over half of Internet users, women's voices and perspectives are not as loud and do not have as much impact online as those of men. Their work demonstrates how some users of the Internet have more agency and can dominate the web, despite the utopian and optimistic view of the web as a socially equalizing and democratic force.[81] Recent research on the male gaze and pornography on the web argue that the Internet is a communications environment that privileges the male, pornographic gaze and marginalizes women as objects.[82] As with other forms of pornographic representations, pornography both structures and reinforces the domination of women, and the images of women in advertising and art are often "constructed for viewing by a male subject,"[83] reminiscent of the journalist and producer John Berger's canonical work *Ways of Seeing*, which describes this objectification in this way: "Women are depicted in a quite different way from men—not because the feminine is different from the masculine—but because the 'ideal' spectator is always assumed to be male and the image of the woman is designed to flatter him."[84]

The previous articulations of the male gaze continue to apply to other forms of advertising and media—particularly on the Internet—and the pornification of women on the web is an expression of racist and sexist hierarchies. When these images are present, White women are the

norm, and Black women are overrepresented, while Latinas are underrepresented.[85] Tracey A. Gardner characterizes the problematic characterizations of African American women in pornographic media by suggesting that "pornography capitalizes on the underlying historical myths surrounding and oppressing people of color in this country which makes it racist."[86] These characterizations translate from old media representations to new media forms. Structural inequalities of society are being reproduced on the Internet, and the quest for a race-, gender-, and class-less cyberspace could only "perpetuate and reinforce current systems of domination."[87]

More than fifteen years later, the present research corroborates these concerns. Women, particularly of color, are represented in search queries against the backdrop of a White male gaze that functions as the dominant paradigm on the Internet in the United States. The Black studies and critical Whiteness scholar George Lipsitz, of the University of California, Santa Barbara, highlights the "possessive investment in Whiteness" and the ways that the American construction of Whiteness is more "nonracial" or null. Whiteness is more than a legal abstraction formulated to conceptualize and codify notions of the "Negro," "Black Codes," or the racialization of diverse groups of African peoples under the brutality of slavery—it is an imagined and constructed community uniting ethnically diverse European Americans. Through cultural agreements about who subtly and explicitly constitutes "the other" in traditional media and entertainment such as minstrel shows, racist films and television shows produced in Hollywood, and Wild West narratives, Whiteness consolidated itself "through inscribed appeals to the solidarity of White supremacy."[88] The cultural practices of our society—which I argue include representations on the Internet—are part of the ways in which race-neutral narratives have increased investments in Whiteness. Lipsitz argues it this way:

> As long as we define social life as the sum total of conscious and deliberate individual activities, then only *individual* manifestations of personal prejudice and hostility will be seen as racist. Systemic, collective, and coordinated behavior disappears from sight. Collective exercises of group power relentlessly channeling rewards, resources, and opportunities from one group to another will not appear to be "racist" from this perspective

> because they rarely announce their intention to discriminate against individuals. But they work to construct racial identities by giving people of different races vastly different life chances.[89]

Consistent with trying to make sense of the ways that racial order is built, maintained, and made difficult to parse, Charles Mills, in his canonical work, *The Racial Contract*, put it this way:

> One could say then, as a general rule, that *white misunderstanding, misrepresentation, evasion, and self-deception on matters related to race* are among the most pervasive mental phenomena of the past few hundred years, a cognitive and moral economy psychically required for conquest, colonization and enslavement. And these phenomena are in no way *accidental*, but *prescribed* by the Racial Contract, which requires a certain schedule of structured blindness and opacities in order to establish and maintain the white polity.[90]

This, then, is a challenge, because in the face of rampant denial in Silicon Valley about the impact of its technologies on racialized people, it becomes difficult to foster an understanding and appropriate intervention into its practices. Group identity as invoked by keyword searches reveals this profound power differential that is reflected in contemporary U.S. social, political, and economic life. It underscores how much engineers have control over the mechanics of sense making on the web about complex phenomena. It begs the question that if the Internet is a tool for progress and advancement, as has been argued by many media scholars, then cui bono—to whose benefit is it, and who holds the power to shape it? Tracing these historical constructions of race and gender offline provides more information about the context in which technological objects such as commercial search engines function as an expression of a series of social, political, and economic relations—relations often obscured and normalized in technological practices, which most of Silicon Valley's leadership is unwilling to engage with or take up.[91]

Studying Google keyword searches on identity, and their results, helps further thinking about what this means in relationship to marginalized groups in the United States. I take up the communications

scholar Norman Fairclough's rationale for doing this kind of critique of the discourses that contribute to the meaning-making process as a form of "critical social science."[92] To contextualize my method and its appropriateness to my theoretical approach, I note here that scholars who work in critical race theory and Black feminism often use a qualitative method such as close reading, which provides more than numbers to explain results and which focuses instead on the material conditions on which these results are predicated.

Challenging Cybertopias

All of this leads to more discussion about ideologies that serve to stabilize and normalize the notion of commercial search, including the still-popular and ever-persistent dominant narratives about the neutrality and objectivity of the Internet itself—beyond Google and beyond utopian visions of computer software and hardware. The early cybertarian John Perry Barlow's infamous "A Declaration of the Independence of Cyberspace" argued in part, "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."[93] Yet the web is not only an intangible space; it is also a physical space made of brick, mortar, metal trailers, electronics containing magnetic and optical media, and fiber infrastructure. It is wholly material in all of its qualities, and our experiences with it are as real as any other aspect of life. Access to it is predicated on telecommunications companies, broadband providers, and Internet service providers (ISPs). Its users live on Earth in myriad human conditions that make them anything but immune from privilege and prejudice, and human participation in the web is mediated by a host of social, political, and economic access points—both locally in the United States and globally.[94]

Since Barlow's declaration, many scholars have challenged the utopian ideals associated with the rise of the Internet and its ability to free us, such as those espoused by Barlow, linking them to neoliberal notions of individualism, personal freedom, and individual control. These linkages are important markers of the shift from public- or state-sponsored

institutions, including information institutions, as the arbiters of social freedoms to the idea that free markets, corporations, and individualized pursuits should serve as the locus of social organization. These ideas are historically rooted in notions of the universal human being, unmarked by difference, that serve as the framework for a specific tradition of thinking about *individual* pursuits of equality. Nancy Leys Stepan of Cornell University aptly describes an enduring feature of the past 270 years of liberal individualism, reinvoked by Enlightenment thinkers during the rising period of modern capitalism:

> Starting in the seventeenth century, and culminating in the writings of the new social contract philosophers of the eighteenth century, a new concept of the political individual was formulated—an abstract and innovative concept, an apparent oxymoron—the imagined *universal individual* who was the bearer of equal political rights. The genius of this concept, which opened the door to the modern polis, was that it defined at least theoretically, an individual being who could be imagined so stripped of individual substantiation and specification (his unique self), that he could stand for every man. Unmarked by the myriad specificities (e.g., of wealth, rank, education, age, sex) that make each person unique, one could imagine an abstract, non-specific individual who expressed a common psyche and political humanity.[95]

Of course, these notions have been consistently challenged, yet they still serve as the basis for beliefs in an ideal of an unmarked humanity—nonracialized, nongendered, and without class distinction—as the final goal of human transcendence. This teleology of the abstracted individual is challenged by the inevitability of such markers and the ways that the individual particularities they signal afford differential realities and struggles, as well as privileges and possibilities. Those who become "marked" by race, gender, or sexuality as other are deviations from the universal human—they are often lauded for "transcending" their markers—while others attempt to "not see color" in a failing quest for colorblindness. The pretext of universal humanity is never challenged, and the default and idealized human condition is unencumbered by racial and gender distinction. This subtext is an important part of the narrative that somehow personal liberties can be realized through

technology because of its ability to supposedly strip us of our specifics and make us equal. We know, of course, that nothing could be further from the truth. Just ask the women of #Gamergate[96] and observe the ways that racist, sexist, and homophobic comments and trolling occur every minute of every hour of every day on the web.

As I have suggested, there are many myths about the Internet, including the notion that what rises to the top of the information pile is *strictly* what is most popular as indicated by hyperlinking. Were that even true, what is most popular is not necessarily what is *most true*. It is on this basis that I contend there is work to be done to contextualize and reveal the many ways that Black women are embedded within the most popular commercial search engine—Google Search—and that this embeddedness warrants an exploration into the complexities of whether the content surfaced is a result of popularity, credibility, commerciality, or even a combination thereof. Using the flawed logic of democracy in web rankings, the outcome of the searches I conducted would suggest that both sexism and pornography are the most "popular" values on the Internet when it comes to women, especially women and girls of color. In reality, there is more to result ranking than just how we "vote" with our clicks, and various expressions of sexism and racism are related.

Algorithms of Oppression

How Search Engines Reinforce Racism

Safiya Umoja Noble

NEW YORK UNIVERSITY PRESS
New York

Stop feeding the hype and start resisting

JANUARY 14, 2023

IRIS VAN ROOIJ

Three weeks ago, I wrote a blogpost about how ChatGPT is a "stochastic parrot" (a term coined by Bender, Gebru, McMillan-Major, & Shmitchell, 2021; see also this video for an explanation) and when used for academic (and other) writing constitutes automated plagiarism. My aim was to bring the discussion down to earth and prevent that hyped-AI hijacks our attention and dictates our education and examination policies.

With disbelief and discontent, I have since watched academics in The Netherlands jumping on the bandwagon and enthusiastically surfing the AI hype wave, e.g., by talking enthusiastically about ChatGPT on national television or in public debates at universities, and even organising workshops on how to use this stochastic parrot in academic education.

Deeply troubled by seeing my Dutch colleages — both at @Radboud_uni and elsewhere in the country — hyping up ChatGPT rather than help curb the hype, which I think is our responsibility as academics. Why do we let money-motivated AI

tech dictate our academic research and debate agendas. We need rather to resist and educate on critical reflection. — (@Iris on Mastodon)

It's almost as if academics are eager to do the PR work for OpenAI (the company that created ChatGPT; as well as its predecessor GPT-3 and its anticipated successor GPT-4).

Why?

The willingness to provide free labour for a company like OpenAI is all the more noteworthy given (i) what is known about the dubious ideology of its founders known as `Effective Altruism' (EA) (Gebru, 2022, Torres, 2021), (ii) that the technology is made by scraping the internet for training data without concern for bias, consent, copyright infringement or harmful content, nor for the environmental and social impact of both training method and the use of the product (Abid, Farooqi, & Zou, 2021; Bender et al., 2021; Birhane, Prabhu, & Kahembwe, 2021; Weidinger, et al., 2021), and (iii) the failure of Large Language Models (LLMs), such as ChatGPT, to actually understand language and their inability to produce reliable, truthful output (Bender & Koller, 2020; Bender & Shah, 2022).

(…) the tendency of human interlocutors to impute meaning where there is none can mislead both NLP researchers and the general public into taking synthetic text as meaningful. Combined with the ability of LMs to pick up on both subtle biases and overtly abusive language patterns in training data, this leads to risks of harms, including encountering derogatory language and experiencing discrimination at the hands of others who reproduce racist, sexist, ableist, extremist or other harmful ideologies reinforced through interactions with synthetic language. — Bender, Gebru, McMillan-Major, & Shmitchell, 2021)

As Tamar Sharon, professor of Ethics and Political Philosophy and co-director of iHub at the Radboud University, notes in the Dutch newspaper NRC[1]: "the ideals of OpenAI are not credible", the company is "founded by millionaires based on their ideology of Effective Altruism, EA" and while they talk about making "beneficial AI", so far this type of tech is realised by exploiting cheap labour of underpaid workers and the push to make Large Language Models (LLMs), such as ChatGPT, larger and larger creates a "gigantic ecological footprint" with implications for "our planet that are far from beneficial for humankind". [quotes translated from Dutch to English, original available in footnote 1].

Why would we, as academics, be eager to use and advertise this kind of product?

Privileged people are left unscathed by the nuanced and system-level issues we touch on (…) these issues are difficult to acknowledge for those in power — they are seen as a sideshow, a political/politicised distraction rather than an essential element of good (computational) science. — Birhane & Guest (2021)

Maybe we, academics, have become so accustomed to offloading our thinking to machine learning algorithms that we cannot think critically anymore (see e.g. Spanton and Guest, 2021; Guest and Martin, 2022; van Rooij, 2020), making us susceptible to believe false, misleading and hyped claims? Or maybe we are afraid to exercise our independent decision making capacity and say "No" to automated bias, hype, misinformation and otherwise harmful technology? Or maybe privileged academics are just fine with enabling the agendas of multimillion dollar companies founded by people motivated by capitalist and bigoted ideologies? Or maybe a mix of these things?

I sure hope not.

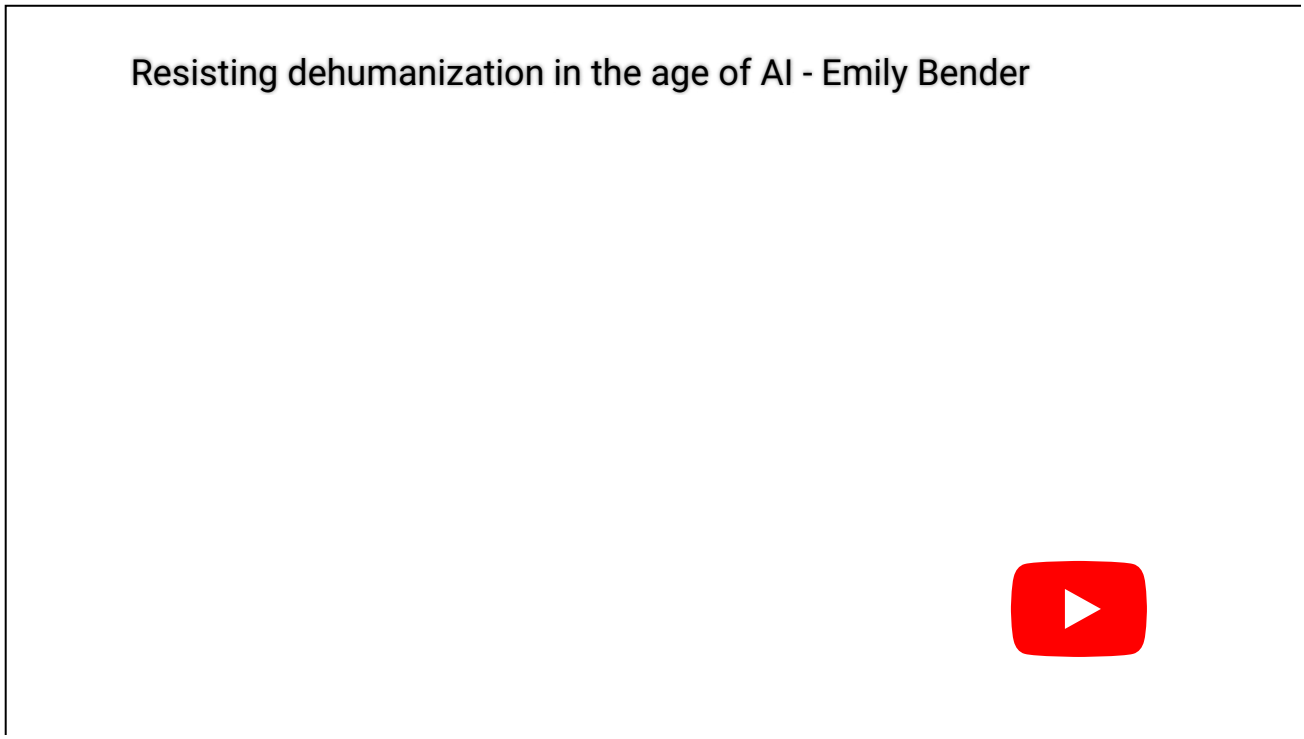
In this age of AI, where tech and hype try to steer how we think about "AI" (and by implication, about ourselves and ethics), for monetary gain and hegemonic power (e.g. Dingemanse, 2020; McQuillan, 2022), I believe it is our academic responsibility to resist.

Academics should be a voice of reason; uphold values such as scientific integrity, critical reflection, and public responsibility. Especially in this moment in history, it is vital that we provide our students with the critical thinking skills that will allow them to recognise misleading claims made by tech companies and understand the limits and risks of hyped and harmful technology that is made mainstream at a dazzling speed and on a frightening scale.

[A]s Safiya Noble warns us in Algorithms of Oppression, these platforms aren't neutral reflections of either the world as it is (…), but rather shaped by various corporate interests. It is urgent that we as a public learn to conceptualize the workings of information access systems and, in this moment especially, that we recognize that an overlay of apparent fluency does not, despite appearances, entail accuracy, informational value, or trustworthiness. — Bender & Shah (2022)

Please join me in resisting and start helping to curb the hype.

As I also said on Twitter and Mastodon, the hype and confusion surrounding ChatGPT is but a tip of an iceberg of the problems caused by AI hype in general. I warmly recommend watching this keynote talk by Emily Bender at last year's Cognitive Science Conference (CogSci2022) to learn more about this topic



Acknowledgements

I am grateful to Olivia Guest for many discussions that have helped me develop a better understanding of some of the issues raised in this blogpost.

References

- Abid, A., Farooqi, M., & Zou, J. (2021). Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 298-306).
- Bender, E.M, Gebru, T. McMillan-Major, A. & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? 🦜. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21).* Association for Computing Machinery, New York, NY, USA, 610–623.
- Bender, E. M., & Koller, A. (2020). Climbing towards NLU: On meaning, form, and understanding in the age of data. In *Proceedings of the 58th annual meeting of the association for computational linguistics* (pp. 5185-5198).
- Bender, E. M. & Shah, C. (2022). All-knowing machines are a fantasy: Beware the human-sounding ChatGPT. The Institute for Art and Ideas.

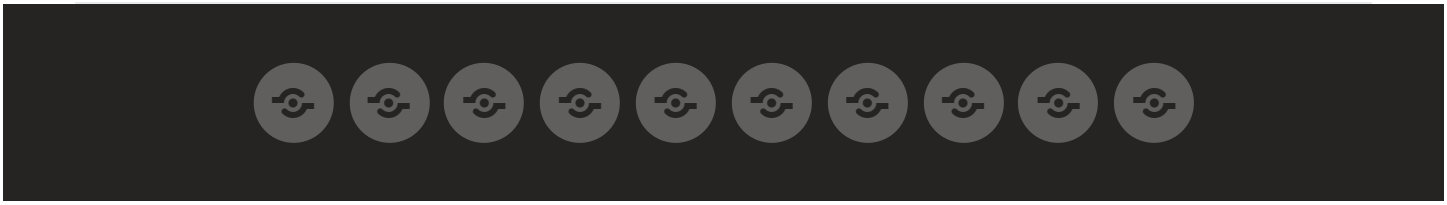
- Birhane, A., Prabhu, V. U., & Kahembwe, E. (2021). Multimodal datasets: misogyny, pornography, and malignant stereotypes. *arXiv preprint arXiv:2110.01963*.
- Birhane, A., & Guest, O. (2021). Towards decolonising computational sciences. *Kvinder, Køn & Forskning*, *29*(2), 60-73.
- Dingemanse, M. (2022). Monetizing uninformation: a prediction. Blogpost on *The Ideophone*.
- Gebru, T. (2022). Effective Altruism Is Pushing a Dangerous Brand of 'AI Safety'. WIRED.
- Guest, O., & Martin, A. E. (in press). On logical inference over brains, behaviour, and artificial neural networks. *Computational Brain & Behavior*. (preprint: https://doi.org/10.31234/osf.io/tbmcg)
- McQuillan, D. (2022). *Resisting AI: an anti-fascist approach to artificial intelligence*. Policy Press.
- Noble, S. U. (2018). Algorithms of oppression. In *Algorithms of Oppression*. New York University Press.
- Spanton, R. W., & Guest, O. (2022). Measuring Trustworthiness or Automating Physiognomy? A Comment on Safra, Chevallier, Gr\ezes, and Baumard (2020). *arXiv preprint arXiv:2202.08674*.
- Torres, E.P. (2021). The Dangerous Ideas of "Longtermism" and "Existential Risk". Current Affairs.
- van Rooij, I. (2020). Mixing psychology and AI takes careful thought. Blogpost in *Donders Wonders*.
- Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P. S., … & Gabriel, I. (2021). Ethical and social risks of harm from language models. *arXiv preprint arXiv:2112.04359*.

Footnote

[1] In Dutch: "*De idealen van OpenAI zijn ongeloofwaardig", vindt [Tamar] Sharon, … "OpenAI is opgericht door een groepje miljardairs vanuit hun ideologie van Effective Altruism, EA (…) Ze hebben het over 'beneficial AI' die in de toekomst menselijke arbeid kan overnemen, maar vooralsnog wordt veel AI aangedreven door menselijke arbeid in lagelonenlanden: tienduizenden onderbetaalde krachten die door de datasets heen spitten. (…) En Large Language Models als ChatGPT hebben een gigantische ecologische voetafdruk: ze slurpen energie. De huidige trend in AI-land is om deze LLM's steeds groter te maken, want daar gaan ze beter van presteren. Wat dat betekent voor de planeet is allerminst beneficial voor de mensheid."– Interview by Colin van Heezik in NRC Handelsblad (1-1-2023).*

PREVIOUS POST
Against automated plagiarism

NEXT POST
Critical lenses on 'AI'



Hybrid Pedagogy

A Pedagogy of Kindness

CATHERINE DENIAL · 15 AUGUST 2019 · CRITICAL DIGITAL PEDAGOGY

In the past two years, when I've been asked to sum up my approach to pedagogy, I've said "kindness."

I didn't always think this way. My graduate education encouraged me to think of students as antagonists, always trying to get one over on their instructors. I was urged to be on the lookout for plagiarism, to be vigilant for cheaters, to assume that the students wouldn't do the reading, and to expect to be treated as a cog in a consumerist machine by students who would challenge their grades on a whim. I was once advised by a senior graduate student to "be a bitch" on the first day of class so that my students never wanted that version of myself to show up again, advice that I dutifully repeated to several of the graduate students who came after me. I was a stickler for deadlines, and memorably once refused to excuse the absence of

a student who was battling a burst pipe in his house when class was in session. I look back on that now and wince.

I gradually learned, through a great deal of trial and error, that this combative way of approaching teaching was counterproductive at best, destructive at worst. Students didn't communicate with me easily, since many of them didn't see the point. They knew (I realize now) that I approached them with suspicion, and so returned that sentiment in kind. It quickly became clear to me that I needed to build relationships, not defensively prevent them from forming, and that trust was a vital part of creating the circumstances under which learning could happen. There was no space for trust to grow in the learning spaces I'd been trying to create, and so I learned to ease up, to let go of rigid control I'd tried to impose upon the classroom, and to make room for the unpredictable and unexpected. I thought, twenty-three years into my teaching career, that I was doing a pretty good job. And then I went to the Digital Pedagogy Lab Institute at the University of Mary Washington in the summer of 2017.

The entire Institute was predicated upon the concept of kindness. From the pronoun buttons available at the registration desk, to the probing questions of the session leaders, to the time people took, one-on-one, to talk about syllabi and assignments, there was an ethos of care running through the whole four days of my residency. I had signed up for the Intro track, and had expected to spend my time evaluating digital tools to bring into my classroom. I did do that, but first I was asked to think about why I needed those tools at all, whom they would serve, and how I would build in accommodations for students with disabilities. My fellow attendees and I were constantly asked to consider why we were doing things the way we were, and what subtextual messages we were sending to our students about who *they* were. I took a good long look at my syllabus, and realized I had communicated everything in it from a position of absolute authority. The language I used to describe the college's Honor Code, for example, expressed the suspicion that everyone was going to commit some awful academic offense at some point, and my attendance policy made no room for the idea that my students were adults with complicated lives who would need to miss a class now and again.

Why? Why did I posit my students as passive novices who couldn't contribute to their own learning? Why did I require students to jump through hoops to prove that they deserved an extension on a paper? Why did I dock points if my students missed three classes in a term? No one had ever asked me to defend my pedagogical choices before, and once they did, I found

much of my pedagogy indefensible. I felt regret and no small amount of embarrassment. My teaching was undone by the presence of a question that was never articulated quite this directly but was everywhere around me:

Why not be kind?

And so I chose kindness as my pedagogical practice. Telling people this has often elicited a baffled response. Kindness is something most of us aspire toward as people, but not something we necessarily think of as central to teaching. In part this is an effect of the pressures that are brought to bear on our classrooms from outside them, symptomatic of a nationwide clamoring (in some circles, at least) for standardization, testing, and rote assessment. Instead of kindness, we're more likely to hear about standards and rigor. (The national professional organization to which I belong says that "good teaching entails accuracy and rigor," but never mentions compassion, for example.) And when we are urged to be kind within an educational setting, it's too often to make up for a lack of institutional support for students and faculty in need, asking a particular service of women and non-binary individuals of all races, and men of color. Kindness can be a band aid we're urged to plaster over deep fissures in our institutions, wielded as a weapon instead of as a balm. And too often people confuse kindness with simply "being nice."

But, to me, kindness as pedagogical practice is not about sacrificing myself, or about taking on more emotional labor. It has simplified my teaching, not complicated it, and it's not about niceness. Direct, honest conversations, for instance, are often tough, not nice. But the kindness offered by honesty challenges both myself and my students to grow. As bell hooks memorably wrote in *Teaching to Transgress*, "there can be, and usually is, some degree of pain involved in giving up old ways of thinking and knowing and learning new approaches."

Yet in practice, I've found that kindness as pedagogical practice distills down to two simple things: believing people, and believing *in* people.

When a student comes to me to say that their grandparent died, I believe them. When they email me to say they have the flu, I believe them. When they tell me they didn't have time to read, I believe them. When they tell me their printer failed, I believe them.

There's an obvious chance that I could be taken advantage of in this scenario, that someone could straight-up lie and get away with it. But I've learned that I would rather take that risk than make life more difficult for my students struggling with grief and illness, or even an over-packed schedule or faulty electronics. It costs me nothing to be kind. My students have not, en masse, started refusing to meet deadlines, but the students who *are* struggling have had time to finish their work. My students have not, en masse, started skipping class, but they're not required to undergo the invasive act of telling me personal details about their lives when they can't show up. My students have not, en masse, started doubting my abilities or my expertise, but they have stepped forward to direct their own education in meaningful and exciting ways that I could not have thought of.

That's believing students. But what about believing *in* students?

Believing in students means seeing them as collaborators — believing they have valuable contributions to make to the way in which syllabi, assignments, and assessments are designed, and life experiences that should be respected in the classroom.

In Fall 2017, I asked both classes to give me questions about the topics we'd be covering — American Indian history in one class, and the history of gender and sexuality in the U.S. in the other. I was then able to craft a syllabus for each class that wove together my own sense of important historical context together with answers to the questions they had posed. The students were offered a sense of ownership in the course, and I was alerted to things I might not otherwise have considered — basic terminology around which there was confusion, for example, or, say, a strong interest in understanding changing concepts of masculinity over time.

I drew on the wisdom of teachers who had gone into this 'kind space' before me, and made significant changes to the way in which I graded work in those classes. Rather than distributing a finished list of grade requirements, I shared some suggestions, and refined those with my students' input until we'd reached a consensus about meaningful assessment. When my students turned in a paper, they also filled out a self-evaluation of their work that asked them what they'd do differently next time, how pleased they were with what they produced, and what they learned about themselves. These adjustments are possible in any class, be it one like mine, with twenty-five students, or a much larger lecture course at a different kind of

institution. Both approaches give students greater ownership over their grade and the way that it's awarded; grading becomes, to whatever degree possible, a collaborative venture. In smaller classes it's possible to go further; my students and I sat together and talked over the answers on their self-evaluation, and I asked my students to give themselves a grade. Together, we entered into a conversation about why that grade felt right to them, and why it did or didn't feel right to me, before reaching a consensus on what grade they'd earned.

I've also begun to think of my classes in terms of universal design. For many years I taught with the idea that there was a well-established, academic norm that was fair and impartial, and my job was to make accommodations available for those students who had particular disabilities, or faced particular challenges in meeting that norm. I no longer believe in such a practice. My job, as I see it now, is to make my classroom accessible to everyone. I've begun the long work of redesigning my lessons and assignments so that everyone is a full participant, and no one needs ask for extra time or a note-taker, because those needs have already been addressed. Because I don't believe students with disabilities should have to out themselves, I no longer ban laptops in my classroom, or have quizzes that some students have to take across the hall to get their necessary time-and-a-half. Instead I've experimented with take-home quizzes, options for students to record videos as well as write papers, and final project guidelines that allow students to create anything that will demonstrate to me what they've learned over the term. This, too, is about belief in my students, and believing that by designing my class to accommodate all types of learning I'm demonstrating something important about the ways in which we should be creating a more just world.

I feel more comfortable as a teacher now than I ever have. The subconscious sense that students were antagonists lingered inside me for a long time — long enough that it has been a marvel to teach these past two academic years and experience a teacher-student relationship without that default expectation. I was less stressed; I didn't have reservations about walking into the classroom. My students rose up to meet every new challenge I presented to them, and vocally affirmed that they appreciated the new approach to grading. Crucially, they articulated that when I looked them in the eye and told them what they had done well in a paper, they believed me, whereas when the same info was written at the end of a paper, they didn't. They saw it as pablum — something that I had to write before I delivered the bad news of what they could still work at (which they interpreted as "what I did wrong.") I see that shift, from their exasperation and disappointment to them becoming partners in the assessment of

their work, was emblematic of the fruits of a pedagogy of kindness. It was, and is, transformational for all involved.

A pedagogy of kindness asks us to apply compassion in every situation we can, and not to default to suspicion or anger. When suspicion or anger is our first response, a pedagogy of kindness asks us to step back and do the reflective work of asking why we're reacting in that manner and what other instances of disappointment or mistrust are coming to bear on a particular moment in a particular student-teacher interaction. This can transform the student-teacher relationship — but it's not only on an individual-to-individual level that it can alter our working world. To extend kindness means recognizing that our students possess innate humanity, which directly undermines the transactional educational model to which too many of our institutions lean, if not cleave. Transactional models of education identify students as consumers and teachers as retail workers who must please their customers (an inhumane model for retail sales as well as the world of learning). Administrators become managers in this model, looking for cents they can save rather than people they can support. This drains the entire system of its humanity, and leads to decisions at every level where the personhood of a student, teacher, or administrator is diminished.

To value and practice kindness is to resist such models. Even where institutions are leaning away from investment in personhood in favor of hedge funds, we as teachers have the ability to insist that individuals matter. We have the means to hold a line, to see the student without shelter — or food, or safety, or a laptop, or an internet connection, or health, or confidence, or a support network — as someone who matters exactly as they are and even because of the challenges they face. We can refuse to dehumanize our students and presume an adversarial stance. We can prioritize kindness.

Published in

critical digital pedagogy • digital pedagogy lab • Kindness • Reviewer: Katheryn Wright • Reviewer: Daniel Lynds • Photo credit: "A Tender Moment" by by Stephanie on Flickr; licensed CC BY-NC 3.0

Publishing

Cheryl E. Ball shares how she blends professional editing, modern publishing, and digital pedagogy to create meaningful courses beyond the classroom walls.

Syllabus-as-Metaphor

We can help — or risk harm — with the metaphors our syllabi embody, and so to serve students as best we can, we must choose our metaphors well.